ТЕМА НОМЕРА

В ПОИСКАХ МУЛЬТИКЛАУДА

ИнформКурьер-Связь
ИКС
издается с 1992 года

Роман Шмаков

Вице-президент подразделения Secure Power в России и странах СНГ компании Schneider Electric

ЦОД: от царства технологий к бизнес-задаче

Реклама

впервые

Международная конференция и выставка

«ЦОД: модели, сервисы, инфраструктура»

23 апреля 2020, Казань, отель «Ривьера»

Темы конференции:

- «Цифровая экономика» как драйвер развития российской индустрии ЦОДов
- Развитие информационной инфраструктуры Республики Татарстан. Планы, перспективы и вызовы
- Требования к ЦОДам для размещения государственных ИС
- Инвестиционная привлекательность отрасли и планируемые меры поддержки
- ИТ- и инженерная инфраструктура современного ЦОДа. Основные тренды
- Edge-ЦОДы. Технологии и решения
- Облачные сервисы в мире и в России. Мультиклауд

При поддержке

Минкомсвязь России

ИННОПОЛИС
Особая экономическая зона

Организаторы

ИКС МЕДИА

iKS CONSULTING

www.kazan.dcforum.ru

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

16+ Реклама

При участии

КООРДИНАЦИОННЫЙ СОВЕТ ПО ЦОДам И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ
Автономная некоммерческая организация

Uptime Institute

Спонсоры и партнеры

3data Premium Data Centers

Western Digital

RITTAL

ZEBC ЭЛЕКТРО

Janitza

C3 SOLUTIONS
КАЧЕСТВЕННО.СДЕЛАНО.В РОССИИ.

ОСК холдинг ОСК ГРУПП

ИМПУЛЬС
ИСТОЧНИКИ БЕСПЕРЕБОЙНОГО ПИТАНИЯ

Ростелеком
ЦЕНТРЫ ОБРАБОТКИ ДАННЫХ

акционерное общество
АБСОЛЮТНЫЕ ТЕХНОЛОГИИ

powerconcept
BATTERY SOLUTIONS

STACK 24 Data Center

Издается с мая 1992 г.

Издатель
ООО «ИКС-Медиа»

участник
АНО КС ЦОД

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

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

Главный редактор

А.Г. Барсков
a.barskov@iks-media.ru

РЕДАКЦИЯ
iks@iks-media.ru

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

Обозреватель
Н.В. Носов
nikolay.nosov@iks-media.ru

Корректор
Е.А. Краснушкина

Дизайн и верстка
Е.В. Денисова

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

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

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

© «ИнформКурьер-Связь», 2020

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

реклама
3data Premium Data Centers
Редакция пользуется облачными услугами 3data

№1/2020 подписан в печать 13.03.20.
Тираж 8 000 экз. Свободная цена.
Формат 64x84/8

ISSN 0869-7973

12+

Альтернативная энергетика неизбежна… и непредсказуема

Новое десятилетие, по крайней мере в развитых странах, пройдет под флагом борьбы за экологию. Она затронет и отрасль ЦОДов. Эксперты предупреждают, что если эта отрасль не станет более активно использовать альтернативную энергетику для удовлетворения своих стремительно растущих потребностей в электричестве, то в 2025 г. будет ответственна за 1/5 всех выбросов углекислого газа. А потребности эти на конец десятилетия, по прогнозу Research Gate, составят 2967 ТВт•ч в год (в 2019 г., по оценкам «ИКС-Медиа», мировая отрасль ЦОДов израсходовала примерно втрое меньше – порядка 900 ТВт•ч).

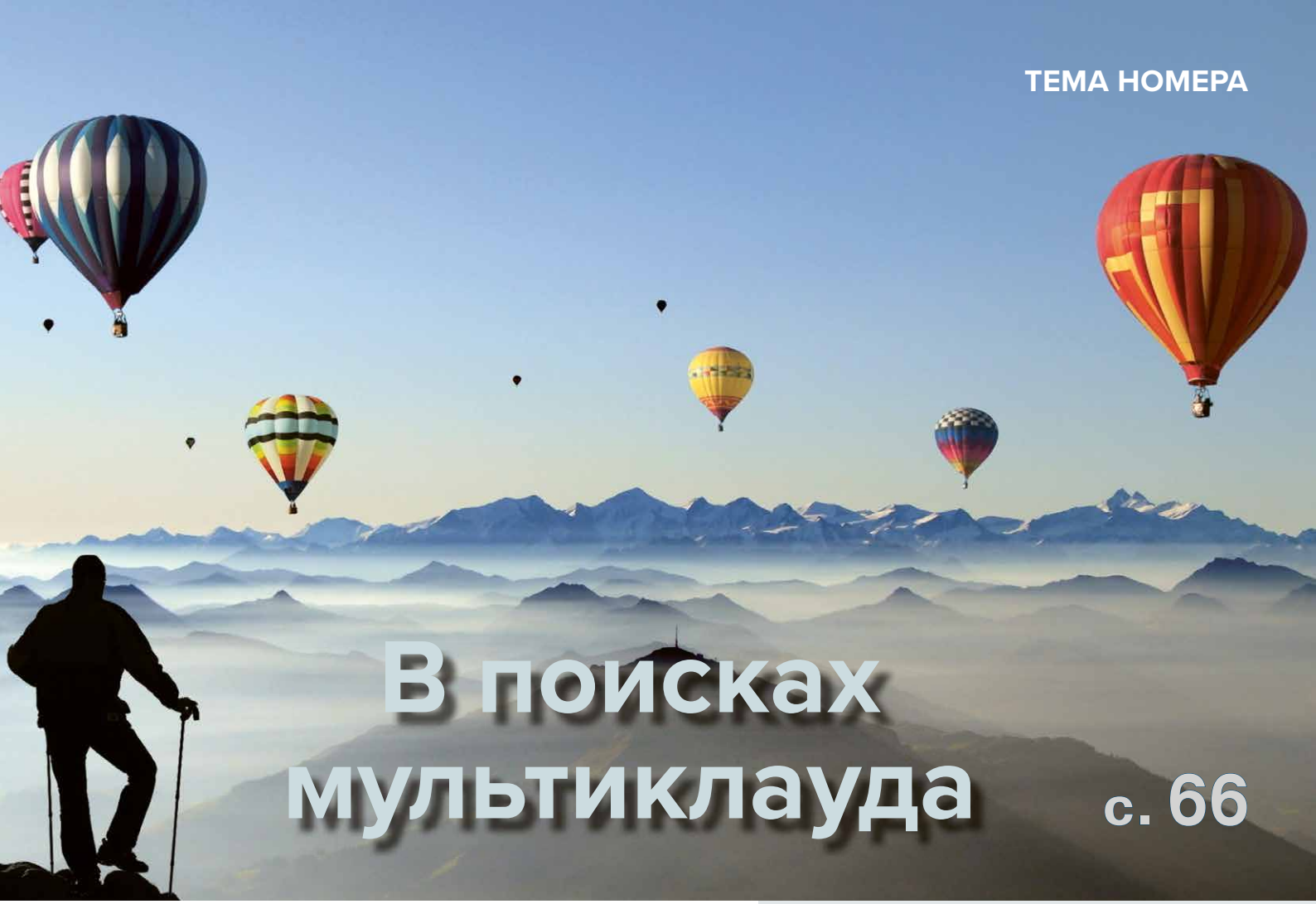
Впрочем, доля альтернативных источников энергии, судя по тем же прогнозам, будет быстро расти. Так, эксперты Vertiv предсказывают, что в 2025 г. 34% всех потребностей ЦОДов в электричестве будут обеспечиваться солнечными батареями и ветровыми генераторами. Аналитики Global Market Insights полагают, что к середине десятилетия построение «зеленых» ЦОДов станет общей практикой, а по крайней мере в США и Европе возобновляемые источники энергии быстро «опередят» традиционные. Катализатором этого станут экологические инициативы развитых стран. Рынок «зеленых» ЦОДов в 2026 г. достигнет $35 млрд, тогда как в 2018 г. он оценивался в $6,5 млрд.

В ответ на призыв ООН спасти планету – Save the Planet – 28 технологических компаний с общей капитализацией $1,3 трлн объявили о согласованном плане не позднее 2050 г. снизить вредные выбросы до нуля. Но многие собираются опередить этот график. Так, Schneider Electric объявила о намерении полностью перейти на возобновляемые источники энергии к 2030 г.

Однако прежде чем переходить на альтернативную энергетику, следует внимательно взвесить все за и против. Например, в Германии ее распространение приводит к ухудшению качества электричества в сетях общего пользования. По мере того как в стране отключаются атомные электростанции и растет доля ветровых генераторов и солнечных батарей, увеличиваются колебания частоты переменного тока в сети.

Получается, что для обеспечения должного качества электричества (которое нужно ИТ-оборудованию в ЦОДах) при внедрении «зеленых» технологий генерации потребуется все больше ИБП с аккумуляторами, производство и утилизация которых, мягко говоря, не самые «зеленые» процессы. Может быть, пока не стоит спешить с отказом от надежных и стабильных традиционных технологий генерации?

За баланс смелых инноваций
и здорового консерватизма,
Александр Барсков



В поисках мультиклауда

с. 66

с. 4

ГИС: в облака, но не в другой регион

с. 12

Т. Толмачева. Как стимулировать инвестиции в цифровую инфраструктуру?

А. Барсков. Пионеры ЦОДостроения. Московская биржа

С. Полухин. Альтернативный «Джокер»: как технологии видеоанализа могли бы спасти Артура Флека

Н. Носов. Кибербезопасность-2019: итоги и тренды

ГИС: в облака, но не в другой регион

Цифровая Россия должна и будет прирастать регионами. Успех проектов создания коммерческих ЦОДов в регионах во многом зависит от привлечения якорных заказчиков и, конечно, инвесторов. Для последних срок окупаемости проекта не должен превышать пяти-семи лет.

Представительной площадкой для обсуждения путей развития ЦОДов в регионах второй год подряд становится конференция, проводимая «ИКС-Медиа» в Екатеринбурге. Ярким фоном конференции стало состоявшееся накануне в столице Урала открытие нового ЦОДа «Ростелекома». Это первый объект столь высокого уровня (дата-центр соответствует требованиям Tier III, но не сертифицирован), построенный компанией за пределами Центрального федерального округа. Более того, это самый крупный коммерческий ЦОД в России за Уралом.

Примечательно, что уже на момент официального открытия все площади объекта (216 стойко-мест) были забронированы заказчиками. Этим фактом посрамлены скептики, утверждающие, что за пределами двух столиц спроса на услуги современных коммерческих ЦОДов нет. Спрос есть и будет расти. Оператору даже пришлось скорректировать свои планы развития проекта: как сообщил Денис Афанасьев, директор по управлению ЦОД компании «Ростелеком – Центры обработки данных» («РТК-ЦОД»), в 2020 г. будет введена в эксплуатацию вторая очередь дата-центра «Екатеринбург» еще на 216 стоек, а в перспективе предполагается довести емкость площадки до 1 тыс. стоек.

В Екатеринбурге пока отсутствуют другие площадки, сопоставимые по емкости с ЦОДом «Ростелекома». По данным iKS-Consulting, следующим по размеру является объект «Филанко» – 52 стойки. Есть еще несколько площадок, по ним у аналитиков нет точных данных, но они определенно меньше.

В 2019 г. на регионы пришлось 16% стойко-мест всех коммерческих ЦОДов России (Москва – 72%, Санкт-Петербург – 12%). При этом, как отметил Станислав Мирин, ведущий консультант iKS-Consulting, с 2017 г. доля регионов уменьшилась на два процентных пункта, что связано с динамичным ростом рынка в Москве, вклад которой в суммарный показатель существенно увеличился. Активного развития рынка в регионах в эти годы не было, но 2020 г. может стать для них переломным.

Надежный якорь

Главная предпосылка для успеха любого коммерческого ЦОДа – наличие спроса. «Важно найти якорного потребителя, который возьмет большую часть мощностей ЦОДа, – считает Павел Ципорин, директор Департамента ИТ и цифрового развития Ханты-Мансийского автономного округа – Югры. – Мы, в частности, ведем активные переговоры с нефтяными компаниями».

Этот тезис подтверждает и пример ЦОДа «Екатеринбург» – более 100 стойко-мест в нем займет компания «Газпром нефть». Причем, как рассказал наш источник в «Газпром нефти», компания давно занималась поисками коммерческого ЦОДа в регионах для создания резервной площадки, но ничего подходящего с точки зрения качества и надежности найти не могла.

Серьезный вызов для индустрии коммерческих ЦОДов в целом и региональных проектов в частности – сломать предубеждение крупных заказчиков, которые предпочитают держать свои ИС и данные у себя. Но ситуация, похоже, меняется. «Мы несколько раз обращались к представителям якорных потребителей, но они не хотели уходить из своих корпоративных дата-цен-




тров. И только в 2019 г. начали проявлять готовность вынести часть данных и систем в коммерческие ЦОДы. В результате нам удалось набрать около 200 стойко-мест потенциальных клиентов», – сообщил Игорь Козодеев, первый заместитель директора Департамента информатизации Тюменской области.

Отсутствие спроса во многих регионах губит экономику проектов. Зачастую окупаемость регионального ЦОДа, по данным, которые привел Видия Железнов, директор по стратегии и маркетинговым коммуникациям «РТК-ЦОД», составляет порядка 10–12 лет. «Это неинтересно инвесторам. Надо существенно улучшить данный показатель», – убежден он.

На это направлены усилия руководителей региональных ИТ-ведомств. «У нас есть льготные земельные участки для строительства ЦОДов, льготные условия налогообложения. Те механизмы для привлечения инвесторов, которые зависят от региональной власти, мы включаем», – рассказал Константин Макаренко, начальник управления технического развития Министерства информационных технологий и связи Челябинской области.

«Предложенные нами меры поддержки сократили срок окупаемости до семи лет. Но это порог, больше уже никому не интересно», – отметил П. Ципорин. В ХМАО – Югре принята стратегия цифрового развития региона, и создание собственного ЦОДа – важная часть этой стратегии.

Где строить

С целью определения приоритетных для построения ЦОДов субъектов РФ создается карта инвестиционной привлекательности регионов («тепловая карта»). «Это будет и документ, и информационная система, – пояснил, выступая на конференции в Екатеринбурге, Игорь Семенихин, директор департамента инфраструктурных проектов Министерства цифрового развития, связи и массовых коммуникаций РФ. – Близость источников энергии, эффективность охлаждения, наличие магистральных каналов связи – эти и многие другие вопросы надо рассматривать в комплексе». 2019 г. ушел на формирование методики, первую половину 2020 г. займет проведение исследования, а вторую – разработка и запуск «тепловой карты».

В качестве места для строительства большого ЦОДа все регионы имеют свои плюсы и минусы, но при этом каждый из них хочет иметь свой дата-центр.

«Мы как самодостаточный регион хотим, чтобы наши ГИСы и данные хранились у нас», – заявил П. Ципорин. Эта позиция хорошо обоснована. Югра – крупнейший нефтегазодобывающий регион, входящий в топ-4 по объему ВРП, в регионе давно и успешно проводят цифровизацию образования, медицины, госуслуг. Высоким уровнем цифровизации характеризуется нефтяная отрасль. В ХМАО уже разработаны концепция и предпроект построения ЦОДа рядом с одной из электростанций.

«Мы не готовы выносить данные из региона, – изложил свою позицию И. Козодеев. – Скажем, colocation в Екатеринбурге или ХМАО нам не интересен. Вариант с облаком в новом ЦОДе «Екатеринбург»? Но тогда нужен канал 20–30 Мбит/с, чтобы эффективно использовать это облако. Мы эгоистично хотим свои ЦОДы, пусть небольшие. Для этого есть готовые индустриальные площадки, есть энергетика, дороги. Правда, надо усиливать каналы связи: наша особенность – малая плотность населения и огромная территория, операторы вынуждены тянуть линии связи на большие расстояния».

В Челябинской области на 2020 г. запланировано строительство первой очереди нового ЦОДа. Всего же, по словам К. Макаренко, в ближайшие несколько лет предполагается открыть один-два коммерческих дата-центра. Стратегия Челябинской области предусматри-

вает активное развитие конечных цифровых сервисов, которые будут стимулировать создание ЦОДов.

Поиском оптимальных мест для новых ЦОДов заняты и московские операторы коммерческих дата-центров. Как рассказал Илья Хала, генеральный директор 3data, компания с помощью iKS-Consulting разработала рейтинг, опираясь на четыре основных параметра: сетевая доступность, деловая активность, открытость, уровень конкуренции. При этом, подчеркнул он, административный фактор, усилия местных администраций также оказывают серьезное влияние на выбор места для новых площадок.

На конференции в Екатеринбурге 3data представила свой проект развития региональных дата-центров по модели франшизы. Одним из многочисленных плюсов такой модели, по мнению И. Халы, является то, что партнер сразу получает возможность предоставлять широкий набор сервисов, наработанных франшизодателем. 3data уже получила несколько десятков заявок от заинтересованных компаний.

Понятно, что далеко не всем регионам нужен не то что мегаЦОД, но даже сравнительно небольшой ИТ-объект на пару сотен стоек. С какого же размера экономически оправдано создание своего дата-центра?

«Мы считаем, что 200 стоек – это минимальный объем. Чем больше ЦОД, тем лучше проявляется эффект масштаба, – отметил Д. Афанасьев. – Но не каждому региону нужен дата-центр даже на 200 стоек, поэтому на рынке есть место и для микроЦОДов и контейнерных решений».

Похожую цифру назвал И. Хала: «Нормальный формат ЦОДа для региона – это 50–300 стоек». Кстати, именно таков размер объектов компании в Москве, где она успешно реализует концепцию дата-центров «шаговой доступности с премиальным уровнем сервиса».

«Мы строим ЦОДы вдоль основных магистральных каналов», – продолжил Д. Афанасьев. Уже в 2020 г. «РТК-ЦОД» планирует запустить в эксплуатацию не только вторую очередь ЦОДа в Екатеринбурге, но и дата-центры в Новосибирске, Санкт-Петербурге, Нижнем Новгороде и Ростове-на-Дону. Общая емкость ЦОДов компании в регионах к концу 2020 г. составит 800 стоек (не считая 2048 стоек дата-центра в Удомле).

ГИСы – в коммерческие ЦОДы

Важным стимулом развития ЦОДов в регионах должен стать перевод информационных систем и информационных ресурсов федеральных органов исполнительной власти и государственных внебюджетных фондов в государственную единую облачную платформу (ГЕОП). Эксперимент по такому переводу уже стартовал, а его исполнителями являются «Ростелеком» и НИИ «Восход». Сформулированы требования к ЦОДам, присоединяемым в рамках этого эксперимента, требования к обеспечению информационной безопасности в ГЕОП, а также к оптимизации архитектуры информационных систем и информационных ресурсов участников эксперимента.

Согласно данным, которые привел И. Семенихин, миграция госсектора в коммерческие ЦОДы принесет на рынок из федерального бюджета порядка 28,6 млрд руб., а это порядка 33% суммарного объема рынка (по данным iKS-Consulting, весь рынок облачных сервисов и коммерческих ЦОДов в 2018 г. составил 87,5 млрд руб.).

Важно, что многие госструктуры «созрели» для того, чтобы выносить свои ИС и данные в облака. «У нас все ГИСы региональных государственных органов уже размещены в нашем региональном дата-центре. Следующий шаг – перевод их в коммерческий ЦОД или в облако», – сказал И. Козодеев.

«Пять лет назад я был не готов выводить ГИСы в облака, – признал П. Ципорин. – Но сейчас поменял свое мнение. Мы будем уходить в облака. Экономика складывается. Это выгодно». В частности, в ХМАО – Югра готовы перенести все 2,5 тыс. рабочих мест госслужащих в облако, причем использовать отечественное ПО.

Создание цифровых АРМов для госслужащих может стать еще одним важным стимулом развития индустрии коммерческих ЦОДов и облачных сервисов. «Это порядка 4 млн рабочих мест. Если они будут предоставляться из облака, значит, деньги, которые раньше выделялись на закупку ПК, пойдут на развитие ЦОДов», – пояснил В. Железнов.

Понятно, что темпы развития ЦОДов в регионах будут определяться их экономическим развитием в целом. Хочется надеяться, что цифровизация регионов будет идти семимильными шагами, тогда и их доля на общем рынке России начнет расти. В любом случае объемы данных будут увеличиваться, и цифровая инфраструктура РФ должна соответствовать этому росту... Если мы не хотим, чтобы наши данные уходили на зарубежные площадки.

Александр Барсков,
Екатеринбург – Москва

Пиринг для облаков

Чтобы выполнить требования национальных программ цифровизации по охвату госструктур, коммерческих предприятий и населения России современными облачными услугами, нужно строить в регионах опорные ЦОДы и развивать сетевую инфраструктуру.

Велика Россия, а ЦОДы строить нужно

Распределение дата-центров по территории нашей страны неравномерно. Большая их часть расположена в столице и ее окрестностях. «73% процента стойко-мест находятся в Москве и ближайшем Подмосковье. Еще 13% приходится на Санкт-Петербург», – отметил директор по развитию бизнеса iKS-Consulting Дмитрий Горкавенко на прошедшем в Москве Пиринговом форуме MSK-IX 2019. Эта неравномерность легко объяснима – как правило, точкой входа в облако является московский офис клиента, да и сбыт продукции чаще всего происходит в столице.

В последние годы ситуация стала меняться. Расширился спектр используемых облачных сервисов, появился спрос из регионов, начали предъявляться определенные требования к времени, проходящему между отправкой пакета по сети и окончанием его обработки (RTT, round trip time). Страна большая, а физику не обманешь. Расстояние между Москвой и Владивостоком по магистралям, проложенным вдоль автотрасс, – более 9 тыс. км, так что, даже задействовав оптоволоконные каналы, RTT меньше 30 мс получить не удастся. Но это в теории, на практике картина хуже. По данным совместного исследования iKS-Consulting и CDNvideo, при работе с облаком, физически локализованным в Москве, RTT во Владивостоке составит 114 мс, в Хабаровске – 106, Якутске – 111, Чите – 81, Иркутске – 71, Красноярске – 53, Омске – 42 мс.

По оценкам iKS-Consulting, если RTT составляет 20 мс, подавляющее число приложений будет функционировать успешно. При задержке от 20 до 40 мс потребуется тщательное тестирование, но, скорее всего, наиболее востребованные сервисы будут по-прежнему работоспособны. При задержках 40–80 мс можно пользоваться только облачными сервисами бэкапа и хранения данных. Граница зоны в 20 мс на востоке и юге страны проходит по Самаре и Ростову. А дальше Красноярска если что-либо из московских облачных сервисов и работает, то это немасштабируемые решения.

Имеющейся сетевой инфраструктуры недостаточно, чтобы соответствовать требованиям, заложенным в национальную программу «Цифровая экономика РФ». Необходимо строительство ЦОДов в регионах. По оценкам iKS-Consulting, чтобы для 90% российских пользователей RTT составляло менее 10 мс, нужно построить ЦОДы в 17 городах, менее 15 мс – в 16.

Строить сеть из полутора десятков ЦОДов долго и дорого. Если же пытаться охватить облачными услугами с приемлемым временем отклика лишь половину российских пользователей, то можно с помощью восьми ЦОДов

снизить задержку до 17 мс. Наилучший вариант их размещения надо выбирать по дополнительным параметрам. Например, по доступности энергетических мощностей, тарифам, наличию ресурсов, коннективности с зарубежными ЦОДами. Даже запуск в оптимально выбранных местах всего четырех ЦОДов уменьшает задержку до 23 мс. «Интеграция каналов и дата-центров – вот то, что открывает окно возможностей для внедрения современных цифровых технологий», – резюмировал Д. Горкавенко.

Строительство ЦОДов в регионах коммерческими компаниями должно быть экономически оправдано. «Основные пользователи сосредоточены в Москве. Экономическая целесообразность выхода в регионы пока под большим вопросом», – заявил директор по развитию бизнеса «Яндекс. Облако» Олег Ковернзев. Компания по-прежнему делает ставку на три дата-центра во Владимирской, Рязанской и Московской областях.

Впрочем, запуск «Ростелекомом» ЦОДа в Екатеринбурге показал, что спрос в регионах есть. Уже на момент запуска вся емкость первой очереди дата-центра была зарезервирована заказчиками, причем сам оператор занял только 10% стоек.

Как обеспечить высокое качество облачных магистралей?

Участники дискуссии «Дорога в облака: зачем нужен хороший транспорт», организованной «ИКС-Медиа», указали, что следует обращать внимание не только на минимизацию задержек, но и на надежность связи. Любой скоростной канал может быть случайно перерезан неквалифицированным экскаваторщиком, и компании должны учитывать такие риски. О. Коверзнев призвал не рассчитывать на показатели надежности ЦОДа, не держать всё в одном дата-центре на одной виртуальной машине, а обеспечивать отказоустойчивость на уровне приложений.

Другой путь – услуги гарантированного подключения к облакам, которые могут предлагаться по сервисной модели с требованиями, зафиксированными в SLA. Такие решения для доступа к наиболее популярным зарубежным облакам уже существуют. «Корпоративный бизнес в основном использует сети MPLS, но сейчас на пятки наступает SD-WAN, и нам в любом случае необходимо обеспечивать хорошую коннективность через публичный интернет к основным облачным платформам и частным облакам», – отметил технический директор российского представительства Vodafone Александр Котов.

Доступ к облакам через публичный интернет может пропасть из-за блокировок Роскомнадзора. В этом случае не поможет резервирование через разных облачных провайдеров. «Если к публичному облаку доступ идет через несколько аплинков, то в случае блокировки все аплинки разрываются, и без использования Direct Connect в него попасть нельзя», – пояснил Евгений Морозов, коммерческий директор MSK-IX.

На RTT влияют не только расстояние до облака, но и топология сети, маршрут транспорта. Для предоставления SLA с хорошими показателями доступности облачного сервиса и RTT оператору следует анализировать задержки на всех маршрутах и физические характеристики трасс.

Важность быстрого и надежного канала до облака возрастает при использовании мультиклаудных технологий. Термин «мультиклауд» эксперты понимают поразному. Одни – как набор лучших приложений из набора облаков, другие – как интегрированную с несколькими облаками систему заказчика. По мнению Е. Морозова, «мультиклауд – это когда сервис настолько важен, что распределен по различным облачным сервисам с целью резервирования». «С развитием PaaS облака будут сильно дифференцироваться по функционалу. В одном облаке можно найти один нужный функционал, в другом – другой. А управление сделать в рамках единой технической политики. В этом случае возникает мультиклауд», – считает коммерческий директор NGENIX Константин Анохин. В зависимости от конфигурации системы клиенту понадобятся канал до частного облака (как правило, выделенная линия), каналы до публичных облаков, от частного к публичным, а в перспективе, возможно, и канал между публичными облаками.

Озабоченность профессионального сообщества вызывает также вопрос о действиях операторов связи в случае установки в каналах технических средств противодействия угрозам в рамках реализации закона о «суверенном интернете». Системы фильтрации трафика (DPI, Deep Packet Inspection) будут находиться под внешним управлением, и непонятно, смогут ли операторы в таких условиях обеспечить выполнение SLA и кто будет отвечать за доступ к облакам.

Закон может отрицательно сказаться и на облачном рынке. Бизнес и так с осторожностью относится к идее размещения в облаке чувствительной информации. При установке в каналах связи систем DPI риски утечек возрастут. Увеличится и RTT – ведь устройствам DPI нужно время на анализ передаваемых данных.

«Часто люди, принимающие решения, не думают о технической реализации. Можно наставить таких ловушек, что никакие облака работать не будут. Будем надеяться, что победят логика и целесообразность», – подвел итог Е. Морозов.

Николай Носов

АПРЕЛЬ

пн	вт	ср	чт	пт	сб	вс
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

МАЙ

пн	вт	ср	чт	пт	сб	вс
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

ИЮНЬ

пн	вт	ср	чт	пт	сб	вс
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

8–10 апреля. Сербия, Белград

Встреча лидеров ИТ-индустрии IT-SUMMIT 2020

АПКИТ

it-summit.ru

14 апреля. Москва

XVI ежегодный международный форум операторов связи «Телеком 2020: новый уровень цифровой трансформации»

«Ведомости»

events.vedomosti.ru/events/telekom20

15 апреля. Москва

Конференция «Умные решения – умная страна»

ГК ЛАНИТ

smart-conference.ru

15–17 апреля. Москва

24-й российский интернет-форум «РИФ+КИБ 2020»

РАЭК

runet-id.com/event/rif20

17 апреля. Санкт-Петербург

Конференция Telecom Day 2020

GlobalNet

telecomday.ru

21–24 апреля. Москва

Российская неделя высоких технологий-2020

Минкомсвязь России, Россвязь, НП «ГЛОНАСС»

hi-techweek.ru

21–24 апреля. Москва

32-я международная выставка информационных и коммуникационных технологий «Связь-2020»

ЦВК «Экспоцентр»

sviaz-expo.ru

22–23 апреля. Москва

13-й международный форум CISO Forum «Музыка кибербезопасности»

Infor media Russia

infor-media.ru/events/67/1767

23 апреля. Казань

Международная конференция и выставка «ЦОД: модели, сервисы, инфраструктура»

«ИКС-Медиа»

kazan.dcforum.ru

23 апреля. Москва

SAP NOW Москва

SAP

sapnow.ru

24 апреля. Москва

4-й российский нефтегазовый ИТ-саммит «Интеллектуальное месторождение»

ЭНСО

itsummit.org

27–30 апреля, Владикавказ

3-я межрегиональная конференция по информационной безопасности «Инфофорум – Северный Кавказ 2020»

«Инфофорум»

infoforum.ru/conference/vladikavkaz-20

20–22 мая. Казань (Иннополис)

Конференция «Цифровая индустрия промышленной России-2020»

ЦИПР

cipr.ru

20–23 мая. Сочи

Конференция российских операторов связи-2020 (КРОС-2020)

NAG

cros.nag.ru

21 мая. Москва

8-я международная конференция Data Center Design & Engineering

«ИКС-Медиа»

dcdeforum.ru

11 июня. Казахстан, Алматы

5-я международная конференция и выставка «ЦОД: модели, сервисы, инфраструктура»

«ИКС-Медиа»

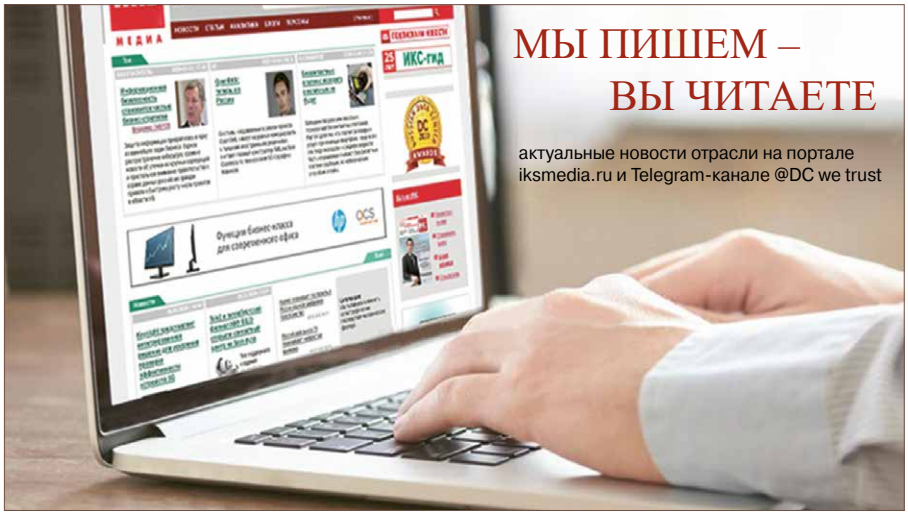
dcforum.kz

16–17 июня. Ханты-Мансийск

4-я международная конференция по информационной безопасности «Инфофорум-Югра 2020»

«Инфофорум»

infoforum.ru/conference/ugra-2020



НОВОСТИ АНО КС ЦОД

НОЯБРЬ 2019. Развитие инфраструктуры ЦОДов на Урале

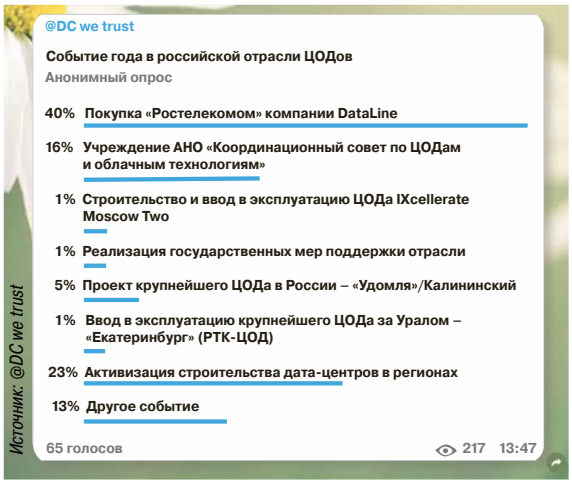
При участии АНО КС ЦОД 28 ноября 2019 г. в Екатеринбурге состоялась конференция «ЦОД: модели, сервисы, инфраструктура», которая собрала ведущих экспертов в области дата-центров, сервис-провайдеров, а также представителей крупных компаний и госструктур Уральского федерального округа. Накануне мероприятия, 27 ноября, «РТК-ЦОД» ввел в эксплуатацию в столице Урала первый ЦОД своей сети, построенный за пределами ЦФО в рамках федерального проекта. *Подробности – на с. 4.*

ДЕКАБРЬ 2019. Заседание Совета АНО КС ЦОД

18.12.2019 прошло заседание Совета АНО КС ЦОД. В состав Совета вошел представитель учредителя АО «Консист-ОС». Также были подведены итоги работы организации за 2019 г., утвержден план деятельности на 2020 г.

ЯНВАРЬ 2020 г. События года российской отрасли ЦОДов

Приобретение «Ростелекомом» компании «Дата-Лайн» – главное событие 2019 г. в российской отрасли ЦОДов. Таковы результаты опроса, проведенного телеграм-каналом @DC we trust среди топ-менеджмента крупнейших отечественных центров обработки данных. В тройку самых значимых событий входят также активизация строительства дата-центров в регионах и учреждение АНО КС ЦОД.



ФЕВРАЛЬ 2020 г.

Проработка мер поддержки отрасли ЦОДов

АНО КС ЦОД были подготовлены и направлены в Минкомсвязь России (по запросу) меры поддержки отрасли ЦОДов в рамках доработки перечня поручений Президента РФ. Предложенные меры нацелены на развитие внутреннего спроса на услуги и повышение инвестиционной привлекательности строительства дата-центров. По ряду мер был подсчитан и представлен экономический эффект.

НОВОСТИ ОТРАСЛИ

«Норникель» построила модульный ЦОД в Москве

Новый ЦОД построен менее чем за три месяца на базе отечественных продуктов. Московский ИТ-кластер обеспечит компании высокую степень производительности и доступности таких систем, как SAP ERP, а также будет служить для резервирования критичных систем, обеспечивающих ее бизнес-процессы. Проект стал финальным элементом комплексной программы «Норникеля» по обеспечению надежности и модернизации ЦОДов, которая проводится с 2015 г. В 2018 г. компания завершила модернизацию четырех ЦОДов в Заполярном филиале и Кольской ГМК.

ЦОД Tier III в Кыргызстане

В Кыргызстане запущен центр обработки данных Национального банка КР. Дата-центр предназначен для выполнения основных задач НБ КР – обеспечения работы платежных и торговых систем, систем межгосударственных платежей и расчетов, получения и обработки банковской отчетности в рамках банковского надзора, системы электронного документооборота, организации обмена информацией через систему электронного межведомственного взаимодействия «Тундук» и т.д. Проект ЦОДа получил сертификат Tier III от Uptime Institute.

Новый министр

21 января 2020 г. главой Министерства цифрового развития, связи и массовых коммуникаций РФ назначен Максут Шадаев. По специальности социолог, М. Шадаев уже работал в Минсвязи – в 2004 г. был назначен советником министра Л. Реймана, с февраля 2006 г. стал директором департамента госпрограмм и развития инфраструктуры, а в мае 2008 г., когда вместо Министерства информационных технологий и связи было создано Министерство связи и массовых коммуникаций РФ, занял в нем пост директора департамента государственной политики в области информатизации и ИТ. С февраля 2014 г. работал министром государственного управления, информационных технологий и связи Московской области. Последняя должность до назначения – вице-президент «Ростелекома» по цифровым платформам.

Linxdatacenter подвела итоги 2019 г.

По предварительным данным, выручка компании выросла на 13%. В 2019 г. компания запустила сервис «Защищенное облако 152-ФЗ», продолжила развитие пула сетевых сервисов ЦОДов Linxdatacenter, а также открыла собственную точку обмена трафиком (IX). Помимо этого, перечень новых услуг Linxdatacenter пополнился сервисом управления контейнерами и услугой утилизации оборудования.

В Московской области запущен дата-центр по франшизе

В рамках регионального развития сети дата-центров 3data активно строятся площадки на территории Московской области, которая входит в число приоритетных регионов географического расширения компании. В конце 2019 г. была реализована первая фаза франчайзингового ЦОДа на территории мультифункционального парка класса A+ Industrial City в подмосковном Сынково. В рамках первой фазы проекта было применено модульное решение, на втором этапе будет построен классический дата-центр с проектной мощностью до 200 стоек.

Региональный ЦОД в Северной Осетии

Компания «Глобал Алания» открыла во Владикавказе ЦОД, в котором будут храниться и обрабатываться массивы данных государственных и коммерческих структур Республики Северная Осетия – Алания. ЦОД спроектирован с учетом требований Tier III. Всего предусмотрено четыре очереди строительства. Планируемая мощность ЦОДа составит 1 МВт, около 100 серверных стоек будут располагаться на площади более 500 кв. м.

ЦОД в Омске

В Омске в районе аэропорта строится современный ЦОД. В июне-июле 2020 г. открывается первый машзал. Всего предусмотрено четыре машзала общей емкостью 150 стоек, мощность электропитания – 1,2 МВт. Объект позволит разместить около 7 тыс. серверов. Инвестором выступает омская компания «Основа Холдинг». Среди будущих клиентов ЦОДа помимо российских есть казахстанские компании.

КОЛОНКА ЭКСПЕРТА

ГАЙ ВИЛНЕР,
соучредитель и генеральный директор IXcellerate

ГОТОВЬТЕСЬ К БУРЕ. КАК КЛИМАТИЧЕСКИЕ ИЗМЕНЕНИЯ ВЛИЯЮТ НА БУДУЩЕЕ ИНДУСТРИИ ДАТА-ЦЕНТРОВ

Не все единодушны в оценке манеры и тона выступления Греты Тунберг в ООН, однако нельзя отрицать, что ее речь стала вехой в дискуссиях вокруг изменения глобального климата, ведь сегодня об этом все чаще говорят за обеденным столом и на отраслевых конференциях.

Когда я думаю об этой экологической проблеме, к моей искренней озабоченности тем, как уменьшить воздействие нашей отрасли на глобальное потепление, присоединяется мысль о том, как сам климат влияет на нашу индустрию.

Как и многие другие профессионалы, считаю, что индустрия ЦОДов должна «готовиться к буре». Климатическая и погодная нестабильность уже сейчас создает экстремальные ситуации, которые мы должны встретить во всеоружии.

Экстремальные погодные условия и такие катаклизмы, как землетрясения и извержения вулканов, всегда учитывались при проектировании дата-центров в рамках планов по обеспечению непрерывности бизнеса. Помню свое удивление, когда еще в начале 2000-х годов увидел, как в Калифорнии укрепляли конструкции ЦОДов с помощью динамических скоб, используя огромные диагональные балки, стягивающие два здания. А совсем недавно я посетил дата-центр в Токио, где все здание площадью 10 тыс. кв. м стоит на восьми резиновых «пончиках», каждый размером с грузовик.

По правилам при выборе площадки для ЦОДа или прокладке оптоволоконной трассы необходимо учитывать максимальный уровень подъема воды при наводнениях и паводках в данной местности за последние 100 лет. Но поскольку погодные рекорды сегодня обновляются всё чаще, возможно, отныне нам придется ориентироваться на более экстремальные значения, чем те, что содержатся в исторических записях.

Во многих случаях соответствующие меры предосторожности уже принимаются. Взять, к примеру, Амстердам. В нем много дата-центров, которые расположены ниже уровня моря, но они чувствуют себя в безопасности, поскольку за ними – сотни лет голландской инженерной мысли и опыта предотвращения наводнений.

Я сознаю, что IXcellerate очень повезло оказаться в Москве, где риск затопления минимален. Однако материковые города, такие как Москва, подвержены риску других катаклизмов, поэтому провести конструктивный анализ здания, изучить фундамент и заказать геоподоснову совершенно нелишне. Несколько лет назад Москва сильно пострадала от торфяных пожаров, смог от которых накрыл большую часть города и заблокировал воздушные фильтры. Также недавно были побиты рекорды максимальной температуры, как летом, так и зимой.

Оборотная сторона медали – это воздействие, которое оказывает на климат наша индустрия. Центры обработки данных, безусловно, потребляют огромное количество энергии, но это лишь ответ на постоянно растущий спрос со стороны конечных пользователей и поставщиков контента. Более того, современные ЦОДы смогли значительно снизить энергопотребление за счет повышения энергоэффективности, сгруппировав тысячи стоек в одном здании вместо того, чтобы размещать их под столами в офисах или в подсобных помещениях, где энергоэффективность почти нулевая.

Конечно же, когда мы об этом говорим, то рассматриваем устройство современного интернета в целом. Действительно, оно не идеально. Мы можем сделать гораздо больше для защиты от непредсказуемых климатических изменений, одновременно сократив спрос на энергию и повысив эффективность ее потребления.

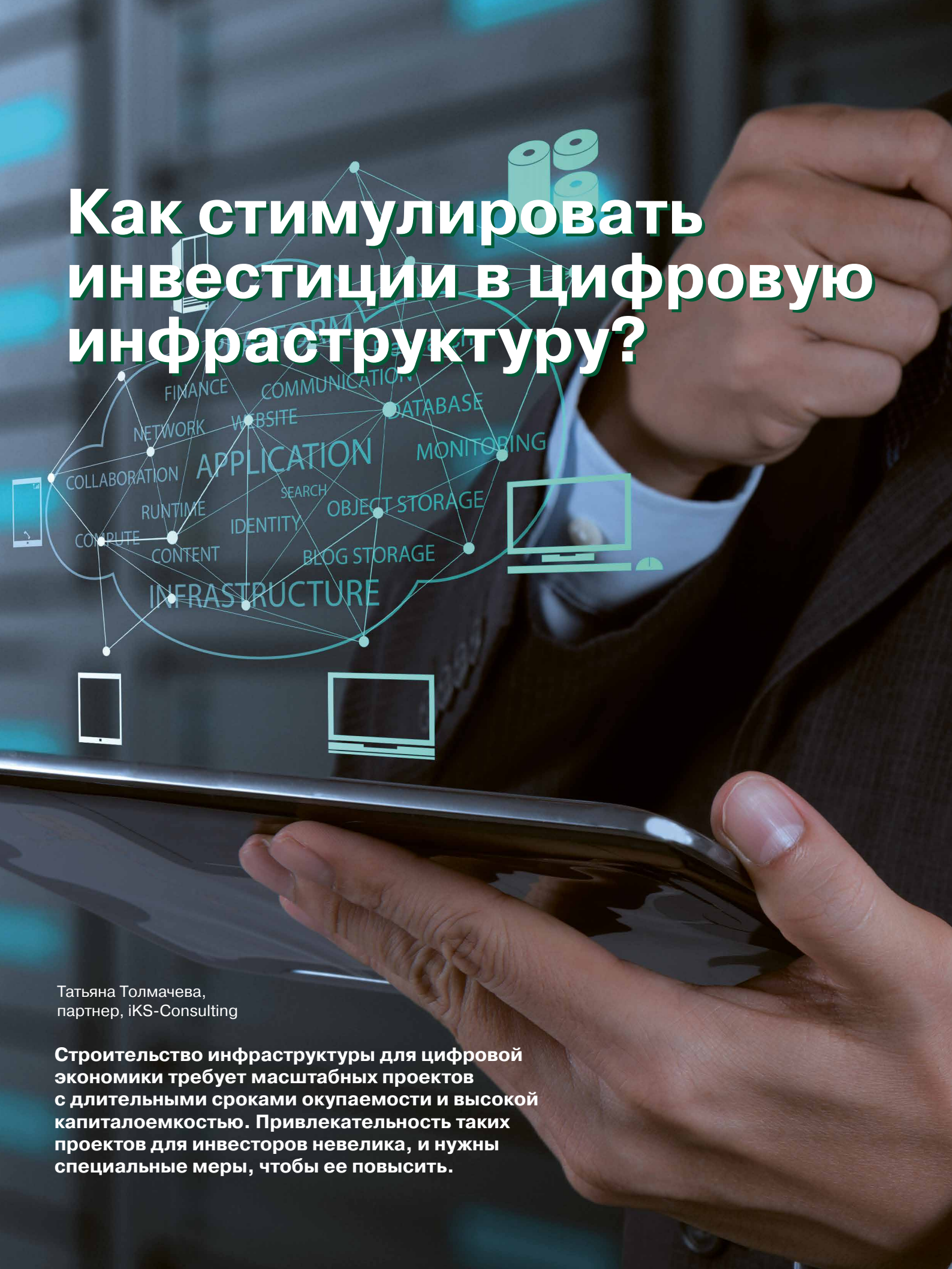
Возобновляемые источники энергии – это то, на чем должны быть сосредоточены все отрасли, и дата-центры могут послужить примером для более широкого их использования. Энергопотребление ЦОДа стабильно, его можно прогнозировать и управлять им, что дает стимулы развитию экопроектов, таких как гидроэнергетика.

Объем энергии, получаемой от таких источников, как солнце, ветер или волны, сильно зависит от погодных условий. Лучший результат, которого можно ожидать от солнечной электростанции, составляет около 20% ее номинальной мощности из-за облачности и сезонных колебаний продолжительности светового дня.

Поэтому массовое накопление и хранение энергии может сыграть важную роль в будущем, в котором доминируют возобновляемые источники энергии, и это действительно способно произвести революцию в энергетической отрасли. Создание в ЦОДах систем сохранения энергии, интегрированных в муниципальную энергосеть, – это очень перспективное направление.

Многие из лучших дата-центров, чтобы сохранять устойчивость к экстремальным климатическим вызовам, проектировались исходя из исторических максимальных показателей. Однако я уверен, что необходим дополнительный анализ, особенно для мест с повышенным риском наводнений или стихийных бедствий. В контексте того, что климатические проблемы стали предметом глобальных дискуссий, я полагаю, что в ближайшей перспективе будет уделяться все более пристальное внимание как воздействию нашей индустрии на климат, так и влиянию климата на инфраструктуру центров обработки данных.

Как стимулировать инвестиции в цифровую инфраструктуру?



Татьяна Толмачева,
партнер, iKS-Consulting

Строительство инфраструктуры для цифровой экономики требует масштабных проектов с длительными сроками окупаемости и высокой капиталоемкостью. Привлекательность таких проектов для инвесторов невелика, и нужны специальные меры, чтобы ее повысить.

Создание цифровой инфраструктуры – одна из ключевых стратегических задач развития Российской Федерации до 2024 г. На расширение сетей связи, системы российских центров обработки данных, внедрение цифровых платформ работы с данными нацелен Федеральный проект «Информационная инфраструктура» Национальной программы «Цифровая экономика РФ». Важным участником и заказчиком инфраструктурных проектов является государство, однако их основной движущей силой остается частный сектор.

Для строительства информационной инфраструктуры в РФ необходимы колоссальные средства. Например, дорожная карта «Технологии беспроводной связи» предусматривает, что в развитие сетей 4G и 5G будет вложено 122 млрд руб. А для того чтобы к 2024 г. достичь запланированной 5%-ной доли на глобальном рынке ЦОДов, потребуются инвестиции не менее 150 млрд руб. Очевидно, что этот объем должны обеспечить частные инвесторы. Как стимулировать частный бизнес вкладывать средства в создание цифровой инфраструктуры?

Один из ключевых показателей инвестиционного проекта, определяющих его привлекательность, – срок окупаемости. Как правило, частные инвесторы идут в проекты, горизонт возврата инвестиций которых составляет 3–5 лет. Вложения в инфраструктуру – это долгосрочные инвестиции, окупающиеся за 7 лет и более. Например, показатель возврата инвестиций на рынке коммерческих дата-центров лежит в диапазоне 8–12 лет. Такие длительные сроки окупаемости предопределяют низкую инвестиционную привлекательность российского рынка КЦОДов. Эффективность вложений очень низка и в проектах обеспечения покрытия мобильной связью удаленных транспортных магистралей или создания объектов связи в отдаленных местностях.

Меры государственного стимулирования инвестиционной активности особенно актуальны при решении задач сокращения цифрового неравенства и подключения к интернету социально значимых объектов, об окупаемости вложений в которые вообще говорить не приходится. Например, дорожной картой проекта «Информационная инфраструктура» в 2020 г. предполагается подключить более 39,5 тыс. СЗО (фельдшерско-акушерские пункты, образовательные организации, органы местного самоуправления, избирательные участки, пожарные части, органы Росгвардии и пр.).

Стимулирование инвестиционной активности в ЦОДостроении требуется в первую очередь в регионах, где инфраструктура коммерческих дата-центров развита слабо. По оценкам iKS-Consulting, на КЦОДы в регионах (исключая Москву, Московскую область и Санкт-Петербург) сегодня приходится чуть больше 16% всех стойко-мест.

От простого к сложному: потребности инвесторов и возможности государства

С позиции инвесторов принцип стимулирования инвестиционной активности в сфере инфраструктурных проектов достаточно прост. Для ее усиления нужны меры, направленные на уменьшение сроков окупаемости проектов до более комфортных для инвесторов и на минимизацию рисков невозврата капвложений. Если за счет дополнительных мер поддержки сроки окупаемости цифровых инфраструктурных проектов сократятся до 5–7 лет, то можно ожидать значительного увеличения частных инвестиций в информационную инфраструктуру.

С точки зрения государства вопрос о мерах господдержки достаточно сложный. Во-первых, государственные ресурсы ограничены (особенно это касается финансов), а значит, есть конкуренция за эти ресурсы между секторами экономики. Во-вторых, всегда существует конфликт между краткосрочными и долгосрочными приоритетами экономической политики. Какой приоритет останется в фокусе – это уже вопрос в том числе политической конъюнктуры. А значит, наличие политического веса у отраслевого ведомства будет играть большую роль.

Очевидно, что приоритеты должны отдаваться мерам, которые могут обеспечить эффективность вложений в крупные инфраструктурные проекты и которые способны изменить структуру экономики. Один из инструментов принятия и обоснования решений о мерах поддержки – оценка влияния капитальных вложений и объемов производства в рамках одного из секторов экономики на народное хозяйство в целом.

Меры государственной поддержки должны давать мультипликативные эффекты, в частности:

- рост производства в секторе;
- дополнительные эффекты за счет межотраслевых связей (рост производства в смежных отраслях);
- увеличение выпуска продукции, сопровождающееся ростом доходов (зарплаты, налоги, прибыль, которые трансформируются в рост потребления/спроса со стороны населения, бизнеса и государства).

Меры государственной поддержки инвестиционной активности могут носить фискальный, финансовый и административный характер. При этом различные комбинации фискальных и

финансовых мер по-разному влияют на изменение сроков окупаемости инвестиционных проектов (примеры таких вариантов для строительства коммерческих дата-центров приведены в таблице).

Как видно, наибольшее влияние на сокращение сроков возврата инвестиций в строительство коммерческих дата-центров оказывают субсидии, льготное кредитование, налоговые каникулы по НДС. Неслучайно эти меры господдержки наиболее востребованы со стороны инвесторов в информационную инфраструктуру. Но одновременно решения по этим мерам принимаются достаточно сложно.

Меры поддержки-2020

Утвержденные дорожные карты на 2020 г. дают представление о мерах экономического стимулирования, принятых Правительством РФ.

Раздел «Меры поддержки» дорожной карты проекта «Информационная инфраструктура» содержит четыре группы мер государственной поддержки:

1. Предоставление льготного финансирования для переоборудования и модернизации производства компаниям, продукция которых имеет статус телекоммуникационного и кабельного оборудования российского происхождения (ТОРП).
2. Снятие административных барьеров в целях повышения экспортного потенциала услуг обработки и хранения данных и облачных сервисов.
3. Обеспечение доступа операторов связи к инфраструктуре многоквартирных домов, изменение порядка оплаты за использование радиочастотного спектра.
4. Финансовая поддержка проектов малых предприятий, занимающихся разработкой и внедрением цифровых платформ.

Уже утверждены правила предоставления субсидий из федерального бюджета на проекты преобразования приоритетных отраслей экономики и социальной сферы на основе внедрения отечественных продуктов на базе сквозных технологий (Постановление Правительства РФ № 1598 от 05.12.2019). Идет отбор технологических проектов для господдержки.

Инвестиции в цифровую инфраструктуру с целью подключения социально значимых объектов будут обеспечиваться из Резерва универсального обслуживания.

Будет ли эффект?

О мерах господдержки развития цифровой инфраструктуры говорится много, но список согласованных и утвержденных мер пока очень скромен.

Наиболее заметны меры, нацеленные на решение задач импортозамещения. Например, льготное кредитование и снижение таможенных пошлин на компоненты, не производимые на территории РФ, смогут получить только компании, продукция которых имеет статус ТОРП. На гранты могут рассчитывать малые предприятия, которые разрабатывают и внедряют цифровые платформы и технологии для них, направленные на развитие информационной инфраструктуры. Все контракты на созда-

Возможные меры господдержки инвестиционной активности и их влияние на сроки окупаемости проектов коммерческих ЦОДов ▶

Мера поддержки	Сокращение срока окупаемости, мес.
Возмещение части понесенных капитальных затрат в проекте строительства ЦОДа	16–18*
Субсидирование процентной ставки по инвестиционным кредитам	
Снижение ставки с 9 до 5%	9–10
Снижение ставки с 9 до 3%	13–15
Обнуление ставки прямых налогов (на имущество, землю и т.д.) для ЦОДа	4–5
Снижение ставки страховых взносов во внебюджетные фонды с 30 до 14%	2–3
Ускоренная амортизация основных фондов (5 лет вместо 10)	
При ставке налога на прибыль 0%	Нет
При ставке налога на прибыль 20%	2–6**
Сокращение сроков согласования проектов строительства ЦОДов в части технологического подключения к энергосетям (итоговое сокращение длительности инвестиционного цикла с трех до двух лет)	6–7
Снижение тарифов на электроэнергию для ЦОДов на 25%	3–4
Каникулы по уплате НДС оператором ЦОДа на 5 лет с момента ввода в эксплуатацию	16–18
Обнуление ставки налога на прибыль с внутренней выручки	8–10
Субсидирование текущей производственной деятельности ЦОДа	14–15***

* При возмещении 20% капзатрат.

** В зависимости от ставок других налогов, прочих факторов, влияющих на прибыль.

*** При субсидиях в размере 10% годовой выручки ЦОДа.

Источник: расчеты Института народнохозяйственного прогнозирования РАН

ние инфраструктуры включают требования по использованию отечественной продукции.

Предполагается, что эти меры будут опосредованно стимулировать развитие рынка для отечественного оборудования связи 5G и инженерной инфраструктуры для центров обработки и хранения данных.

Стоит отметить, что на текущий момент индустрия ЦОДостроения не входит в число 22 приоритетных отраслей, включенных в программу импортозамещения. Вместе с тем ожидается, что в перспективе часть наработок данной программы будет задействована для решения задач рынка ЦОДов. Но эффект будет иметь отложенный характер. Экономическая политика, нацеленная на импортозамещение, важна для развития российской экономики в целом. В проектах же строительства ЦОДов как инженерных объектов основными выгодоприобретателями являются зарубежные производители оборудования, а мультипликативные эффекты для отечественной экономики незначительны. Так, капитальные затраты на строительство ЦОДа в пересчете на одно стойко-место составляют в среднем $30–50 тыс., и из них почти 50% приходится на инженерные системы – чаще всего импортного производства.

Законотворческая деятельность, доработка регулирующих документов под требования развития цифровой экономики также играет важную роль для выполнения федеральных проектов строительства информационной инфраструктуры. Она позволяет снимать риски инвестиционных проектов, снижать административные барьеры, в некоторых случаях – сокращать сроки окупаемости проектов.

Но, как показал 2019 г., даже согласование законодательных мер государственной поддержки – процесс долгий и болезненный. Основная проблема, по нашему мнению, заключается в характере межведомственного взаимодействия и конфликте ведомственных интересов. Например, при выделении радиочастотного спектра для систем связи 5G Министерство обороны заняло особую позицию. Схожий по остроте вопрос – взаимодействие энергетиков и операторов связи, операторов дата-центров. Энергетики до сих пор не рассматривают провайдеров информационной инфраструктуры как крупных потребителей электроэнергии, часто игнорируют их интересы. Так, не получило согласования и было исключено из мер поддержки на 2020 г. упрощение процедуры выхода на оптовый рынок электроэнергии телекоммуникационным компаниям для целей взаимодействия с субъектами оптового рынка электроэнергии. Зато инициатива Минэнерго ввести плату за неиспользуемый резерв энергомощности может дать прямо противоположный эффект – увеличит срок окупаемости проектов строительства коммерческих ЦОДов.

Можно ожидать, что дорожные карты, утвержденные на 2020 г., будут реализованы, а согласованные меры поддержки начнут работать. Но я полагаю, не стоит рассчитывать, что эти меры окажут значительное влияние на рынок информационной инфраструктуры, даже в долгосрочной перспективе.

«Совершить настоящий прорыв в цифровизации реального сектора» – к чему призвал, выступая в Госдуме, премьер-министр – с такими мерами, скорее всего, не удастся. А смена правительства на какое-то время заморозит все дискуссии по поводу согласования и принятия других мер господдержки развития информационной инфраструктуры. ИКС

Региональный ЦОД как драйвер роста и диверсификации экономики

ХМАО – Югра входит в число передовых регионов России в вопросах цифрового развития. Создание регионального дата-центра может стать катализатором для привлечения в округ бизнеса, основанного на данных, стимулом к росту региональной интернет-экономики.

Ханты-Мансийский автономный округ – Югра входит в топ-5 субъектов РФ по уровню цифровизации (индекс «Цифровая Россия», 2018). Недавно губернатор Югры Наталья Комарова выступила с инициативой создать в регионе парк дата-центров, который войдет в федеральную сеть опорных ЦОДов и обеспечит доступность услуг хранения и обработки данных для граждан, бизнеса и власти на всей территории автономного округа. Идея была поддержана Министерством цифрового развития, связи и массовых коммуникаций РФ.

Югорский научно-исследовательский институт информационных технологий (ЮНИИ ИТ) как организация, созданная Правительством Югры для обеспечения социально-экономического развития региона и внедрения информационных технологий в производственную и социальную сферы округа, играет важную роль в проекте строительства регионального ЦОДа. Об этом и о других проектах цифрового развития в Югре мы беседуем с директором ЮНИИ ИТ, доктором технических наук Андреем Витальевичем Мельниковым.

– Андрей Витальевич, частные инвесторы при финансово-экономическом обосновании проекта строительства ЦОДа в первую очередь спрашивают о потенциале и возможности утилизации мощностей нового дата-центра в соответствии с бизнес-планом. С другой стороны, мы часто слышим, что в регионах нет или почти нет спроса на инфраструктуру хранения и обработки данных. Вы согласны с таким мнением?

– Так говорят те, кто считает, что за границами Москвы жизни нет ☺.

Если серьезно, конечно, не согласен. Югра – крупный экономический центр. Кстати, всего в трех часах лета от Москвы. ХМАО входит в первую четверку субъектов РФ по объему ВРП. В 2019 г. он вошел в топ-5 регионов с высоким текущим уровнем экономического «здоровья» и положительной экономической динамикой. Конечно, Ханты-Мансийский автономный округ имеет свою ярко выраженную специфику. В регионе проживают чуть более 1,6 млн жителей (в силу его особых климатических условий), и при этом он является крупнейшим нефтегазодобывающим регионом не только в России, но в мире. Более 60% ВРП приходится на добычу полезных ископаемых. На территории округа ведут хозяйственную деятельность более 50 нефтегазодобывающих предприятий.

Мы видим, что в регионе есть серьезные потребности в инфраструктуре центров обработки и хранения данных. Правда, текущие потребности пока закрываются мощностями собственных (корпоративных и ведомственных) ЦОДов. Одновременно мы видим тенденцию миграции корпоративных и ведомственных дата-центров в коммерческие ЦОДы. Таких примеров достаточно много.

– Наблюдаете ли вы дефицит инфраструктуры коммерческих ЦОДов в УФО?

– Как я уже сказал, текущие потребности закрываются корпоративными и ведомственными ЦОДами.

Тем не менее в горизонте трех-пяти лет дефицит инфраструктуры для хранения и обработки данных в регионе однозначно проявится. И для этого есть две причины. Во-первых, во всех экономических и социальных сферах активно реализуются федеральные и региональные программы цифровизации, которые предполагают перевод всех данных о гражданах и бизнесе в «цифру», внедрение АИС во многих секторах экономики и общественной жизни.

Во-вторых, сегодня мы видим, что требования к дата-центрам повышаются. Не все организации и предприятия смогут обеспечить соответствие различных параметров эксплуатации ЦОДа современным требованиям. Ожидаем, что многие региональные органы власти постепенно будут переходить на инфраструктуру коммер-

ческих ЦОДов. К этому будет подталкивать вся государственная политика в сфере развития информационной инфраструктуры.

Мы понимаем, что уже сейчас нужно готовиться к росту потребностей в инфраструктуре хранения и обработки данных со стороны как региональных органов власти, так и регионального бизнеса.

ХМАО – самодостаточный регион, может позволить себе поддержать инвестиционные проекты, стратегически важные для его развития. Тем более что перед округом стоит задача снижения зависимости региональной экономики от нефтедобывающего комплекса. Построение инфраструктуры хранения и обработки данных может стать катализатором для привлечения в округ бизнеса, основанного на данных, стимулом к росту региональной интернет-экономики.

Руководство округа готово поддержать частных инвесторов, которые придут к нам в регион, чтобы построить региональный ЦОД.

– Наблюдаете ли вы рост потребности нефтегазодобывающих компаний в современной инфраструктуре ЦОДов в нефтегазоносных регионах? Почему вы думаете, что эти компании станут клиентами нового регионального ЦОДа?

– Повторюсь, наш округ – один из крупнейших нефтегазодобывающих регионов. Наш институт успешно сотрудничает со многими компаниями нефтегазового сектора. Например, Центр геологического моделирования института совместно с ООО «Технологический центр «Бажен» (ПАО «Газпром нефть») разрабатывает подсистему математического моделирования цифровой платформы в рамках проекта «Бажен».

Совместно со специалистами «Нижневартовск-НИПИнефть» (ПАО «Роснефть») в институте разрабатывается программное решение «Система оптимизации размещения кустовых площадок в условиях подземных и поверхностных ограничений». Кроме того, ведутся работы по созданию информационной системы расчета и планирования капитальных затрат при освоении месторождений.

Мы понимаем ИТ-потребности нефтяных компаний. Видим, как автоматизируются предприятия нефтегазодобывающей отрасли, какие у них планы внедрения современных методов интеллектуального управления добычей трудноизвлекаемых запасов нефти, моделей управления нефте- и газодобывающими предприятиями в соответствии с концепцией «Индустрия 4.0».

Логично, что новый региональный ЦОД будет учитывать специфику и потребности нефтегазодобывающих компаний. Например, обеспечивать непрерывное функционирование программно-аппаратного обеспечения, защиту информации при передаче данных, защиту от несанкционированного доступа и пр.

Мы сознаем, что все крупнейшие нефтегазодобывающие компании имеют либо собственные, либо кэптивные дата-центры. Но региональный ЦОД сможет обеспечить потребности нефтяных компаний в хранении, обработке и анализе геолого-геофизической и промысловой информации. Например, в 2012–2019 гг. в округе пробурено 32 720 скважин, из них 3700 – в 2019 г. В период с 2012 по 2018 гг. в регионе «отстрелено» 26 682 погонных километра 2D-сейсморазведки и 33 855 кв. км сейсморазведки 3D. При этом объем полевой информации, получаемой с площади 100 кв. км, составляет примерно 30–40 Гбайт. С внедрением высокоплотной сейсморазведки 3D объем информации вырастет на порядок.

Региональный ЦОД сможет также обеспечить сбор и хранение возрастающего объема данных от «цифровых» скважин, обусловленного тенденциями их цифровизации и переходом от технологии единичных периодических измерений к непрерывному мониторингу промысловых и геофизических параметров.

– На ваш взгляд, потребности в инфраструктуре ЦОДов в ХМАО аналогичны таким потребностям в других регионах?

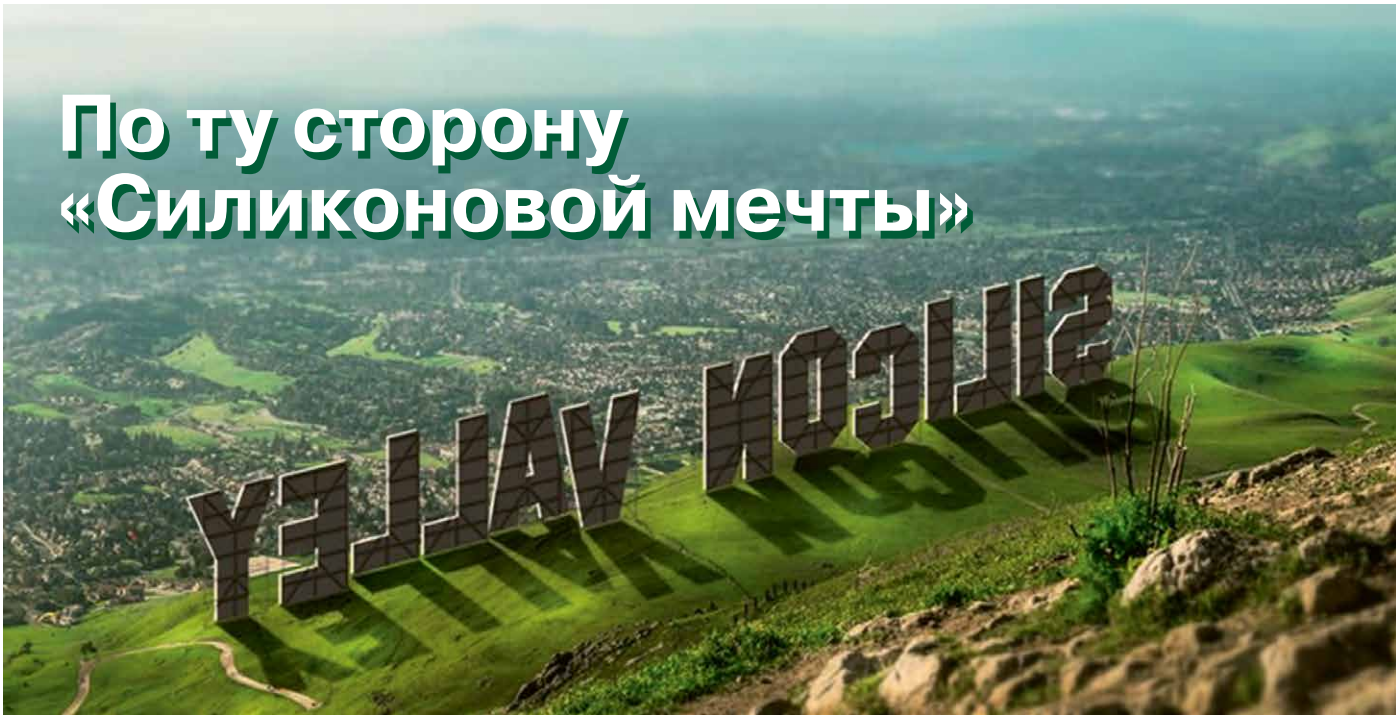
– Каждый регион уникален. Тем не менее в части цифровизации государственного управления и цифрового взаимодействия с гражданами и бизнесом потребности будут схожи. Каждый регион должен будет внедрить/модернизировать региональные автоматизированные информационные системы «Здравоохранение», «Образование», ЖКХ, «Безопасный город», ЗАГС, «Правосудие» и пр. Постепенно все эти системы будут переноситься либо в облако (по концепции ГЕОП), либо в инфраструктуру коммерческих дата-центров (по концепции сервисной модели потребления). Эти процессы и поддержат спрос на физическую и вычислительную инфраструктуру ЦОДов в регионах.

– Расскажите немного о проекте. На каком этапе находится его реализация?

– Мы сейчас находимся на стадии привлечения в проект частных инвесторов. У проекта есть финансовая и административная поддержка регионального правительства, есть возможность привлечь льготное финансирование институтов развития. Но для коммерческого успеха проекта необходимо, чтобы пришла команда предпринимателей с опытом развития аналогичного бизнеса и/или частных бизнес-ориентированных инвесторов. Интерес к проекту высокий. Идут переговоры. Приглашаем всех заинтересованных инвестиционных партнеров.

Беседовала Татьяна Толмачева

По ту сторону «Силиконовой мечты»



Игорь Бакланов

Трудно не признать, что отдача от инвестиций в науку и научно-прикладную деятельность в России более чем скромная. Однако ошибки, допущенные при формировании нашей научно-инвестиционной системы, сделали такой результат закономерным.

В нашем профессиональном сообществе мечта о «Силиконовой долине» сродни California Dream для среднего американца, это надежда на светлое будущее. Мы знаем, что наша отрасль – системы связи и ИТ – находится в состоянии научно-технической революции. В повседневной жизни мы видим достижения этой самой революции – новые скорости, гаджеты, машинное обучение, нейронные сети, наконец, искусственный интеллект. Современный работник отрасли – от программиста до системного архитектора – воспринимается окружающими, как атомный физик середины 20 века. Вызывает уважение, с налетом тайны и секретности, поскольку все равно непонятно, чем занимается. Но непременно революционно. Мы жаждали этой революции. Каждый из нас в глубинах сознания понимал значимость нашего дела и своего места в нем.

Еще десять лет назад мы все были Стивами Джобсами и Биллами Гейтсами разного масштаба. Мы хотели развить виртуальную реальность, построить цифровую экономику, приручить мощь компьютерных систем и все это принести в дар своей стране, компании, семье – всему миру. Мы чувствовали гордость от того, что мы – инженеры новой эпохи, никак не этапа, а именно эпохи. Компьютерные технологии формировали уникальный технико-гуманитарный дискурс, которого до сих пор не знала человеческая цивилизация. И мы хотели, чтобы этот мир технологий был нашим, российским, советским – не важно, кто как это называл.

Прообразом этой новой эпохи все считали Кремниевую долину в Калифорнии – средоточие всех значимых компаний, настоящую Мекку современных компьютерных и информационных технологий. Чтобы как-то выделить это место, его название специально переводили неправильно – Силиконовая долина. Совершая туда паломничество, мы грезили, что и у нас, в России ЭТО БУДЕТ. Так формировалась наша профессиональная «Силиконовая мечта».

Как грибы после дождя, начали прорастать в России инновационные фабрики, технопарки, стартапы, коворкинги – все то, что соответствовало «Силиконовой мечте». Появились инвесторы, инноваторы, бизнес-ангелы.

Но прошло десятилетие... и ничего. Несмотря на НТР, на выставке «Экспокомм» показать нечего, да никто туда уже и не ходит. Строительство инновационных фабрик обернулось коррупционными скандалами. Освоенные миллиардные средства дали самые скромные результаты. Государство распорядилось, чтобы новые сети 5G создавала корпорация «Ростех», объединяющая государственные предприятия, – они по крайней мере сохранили советские техноло-

гии. Инноваторы и инвесторы часто оказываются нечистоплотными и сейчас добивают даже то, что выросло на энтузиазме и вопреки «инновационному климату». Достаточно посмотреть на судьбу аналитического портала Banki.ru и его создателя Филиппа Ильина-Адаева. Или на судьбу первого русского софтсвича «Мера» и вспомнить добрым словом покойного Игоря Масленникова.

Можно сказать, что нас предали, что казнокрады в очередной раз освоили бюджеты. Что нашу мечту превратили в «тему» и вырастили на ее основе «инновационные пилорамы».

Но так ли все просто в инновационном мире?

Научно-инвестиционные системы

Давайте зададимся простым вопросом: откуда взялись инновационные фабрики? Ведь не на пустом месте они выросли. Кто заложил основы современной российской инновационной отрасли и принципы руководства наукой и научно-прикладной деятельностью?

Из анализа истории и документов складывается интересная картина. В середине 90-х в российской экономической литературе появился и в 2000-е рядом политических экономистов усиленно развивался термин «научно-инвестиционная система» (НИС). Следует отметить, что в литературе того периода о НИС писали много, но ни одного инженера или ученого неэкономического профиля в авторах публикаций по НИС найти не удалось. НИС в России развивали экономисты и финансисты. Упор во всех публикациях делался на технологии управления инвестиционной и научно-инвестиционной деятельностью.

Возникновение проблематики НИС естественно: Россия от социалистической экономики перешла к построению капиталистического общества. Советская наука и методы управления ею в новую экономику капитализма не вписывались и начали разрушаться. Тогда появился закономерный спрос на разработку модели управления научной и инвестиционно-технической деятельностью в условиях капитализма. Вот и родилась идея создания НИС как части новой экономики.

Кто должен был построить научно-инвестиционную систему для новой экономики России? Формальная логика требует привлечения ученых (от науки), финансистов (от инвестиций) и экономистов (НИС – это часть капиталистической экономики). Ученых решили «оптимизировать», поскольку есть ученые-финансисты и ученые-экономисты. Вот эти две группы и создавали российские стандарты НИС.

Сегодня можно подвести краткие итоги десятилетнего применения разработанной в нулевые российской модели НИС:

- в нашей стране существует огромное количество фондов, инновационных долин, технопарков, программ поддержки инноваций, но КПД всего этого многообразия более чем скромный;
- мы не наблюдаем появления новых российских брендов. Наоборот, уже состоявшиеся компании банкротятся и исчезают;
- разрушены система высшего практического образования и отраслевые направления технических наук;
- исчез институт главных конструкторов, исчезают просто конструкторы;
- ощутимо снизился уровень инженерной школы;
- и, самое главное, нет ощутимых результатов.

Оценивая состояние российской НИС, можно сказать, что проект оказался неудачным. Открытым остается вопрос, являются ли причины неудачи сугубо субъективными («опять все разворовали!») или же они объективны.

Неудачная копия «Силиконовой долины»

Активное обсуждение тематики НИС в нулевые годы не вышло за границы экономического и финансового профессионального сообщества. Это оказалось главной ошибкой самого процесса разработки НИС – ее просто решили скопировать с Кремниевой долины. Это видно по характеру публикаций – они носили сугубо описательный характер, никакого критического и многофакторного анализа не проводилось.

Скорее всего, в калифорнийскую Кремниевую долину был высажен «десант» экономистов и финансистов, чтобы через курсы обучения, совместные проекты и взаимные презентации узнать, «как у них там все устроено», и сделать так же, как в ведущей экономике мира. «Десантники» накопили знания, которые проросли сначала публикациями и диссертациями экономического и финансового профиля, а потом уставами различных форм инновационных фабрик, федеральными целевыми программами и пр.

Но в процессе копирования не учитывались исторические и культурные особенности наших народов. Эти особенности, подводная часть айсберга американской и европейской НИС, не были учтены экономистами и финансистами вследствие профессиональной узости взглядов. Создатели российской НИС их просто не заметили. А различия радикальные:

- В вузах, начиная со студенческих клубов и спортивных команд, формируются профессиональные сообщества с личными связями. В дальнейшем эти связи становятся основой доверительных отношений между участниками рынка (выпускники вузов оказываются в разных орга-

низациях, но сохраняют личные связи). Отсюда возникает персональная ответственность за исполнение обязательств. Нарушивший «кодекс чести» вуза подписывает себе смертный приговор как профессионал.

◪ Западное общество пронизано протестантской этикой, имя и честь специалиста, его профессиональная репутация в научных и технических кругах не пустой звук, и это также является гарантией персональной ответственности.

◪ Параллельно с НИС действуют не участвующие в ней профессиональные команды, а также специальные аналитические агентства, имеющие сопоставимую ценность.

То есть существуют «официальная» и «неофициальная» части НИС. При заимствовании «неофициальная» часть НИС не учитывалась.

Ну и главное отличие России от развитых стран Европы и Америки – совершенно другой уровень капиталистических отношений в системе экономики. Наш капитализм не может рассматриваться как зрелый, он проходит стадию 19-го века, а не 20-го, не говоря уже о 21-м.

Все перечисленное привело к методическим ошибкам в построении современной российской НИС:

☒ Она является заимствованием из структур западных экономик и ориентирована на развитую промышленность, тогда как экономика России находится в состоянии кризиса высокотехнологичных отраслей.

☒ В НИС доминирует подход на основе процессов (процессов контроля, управления, финансирования и пр.), что развивает ее в направлении «процесс ради процесса», создавая почву для бюрократизации.

☒ Различие культур Запада и России не позволяет использовать такие компоненты НИС Запада, как протестантская этика, авторитет alma mater, влияние университетских клубов и связей, а также профессиональных сообществ – структур, которые обеспечивают режим доверия и персональной ответственности в НИС Запада. Этическая компонента в НИС России заменена системой контроля и предотвращения мошенничества, что еще более ее бюрократизирует. Современный инвестиционный проект на 90% сосредоточен на доказательстве того, что деньги не будут «выведены» на непрофильную деятельность, и на системе контроля, которая делает сам творческий процесс невозможным.

☒ Отсутствие механизма обеспечения доверия в НИС России приводит к требованиям доказательств востребованности разработки и/или быстрого коммерческого эффекта (соинвестирование, коммерциализация, государственно-частное партнерство в разных видах и пр.), что подрывает саму идею инвестиций. Долговременные и фундаментальные проекты в такой системе вообще невозможны.

☒ Вопросы результативности, наращивания опыта, разработки технологий в НИС вторичны по отношению к процедурным процессам, поэтому она оказывается безрезультатной или имеет низкий КПД.

Бюрократизм в сочетании с отсутствием механизма обеспечения доверия обрекает современную российскую НИС на самодостаточность, превращает в процесс ради процесса, без результатов.

Советская НИС

Интересно, что в нашей истории есть образец успешной НИС, а именно советская научно-инвестиционная система. Перечислим голые факты, связанные с «космическим проектом» как наиболее интересным, поскольку он был построен с нуля и в обстановке совершенной научной и технической неопределенности.

★ В 1945 г. закончилась Великая Отечественная война.

★ Страна унаследовала фрагменты (чертежи, часть производства, несколько специалистов) проекта ФАУ-2.

★ За 10 лет были созданы научная, инженерная, производственная школы, разработана технология ракетостроения.

★ В 1957 г. в СССР запустили первый спутник, обозначив доминирование наших технологий в космонавтике на следующие 30–40 лет: более 3 тыс. предприятий, сотни тысяч инженеров, специальности, технологии, научные достижения.

★ Все это было сделано в условиях фактически разрушенной войной страны, бедствующего населения.

Сравнение эффективности советской НИС с сегодняшними российскими и даже американскими реалиями может рассматриваться как доказательство победы социализма над капита-

лизмом в области современных технологий и инноваций.

Но заимствовать советскую НИС в современной экономической ситуации России невозможно, для этого требуется как минимум вернуть социализм, восстановить партию, Госплан и воспитать новое поколение «строителей светлого будущего», которые в свое время и создали советскую НИС.

Открытые вопросы создания российской НИС

Налицо объективный кризис управления экономикой:

- Созданная в России НИС доказала свою неработоспособность. В силу методических ошибок ее разработчиков никаких других результатов быть и не могло.
- Вернуться к советской НИС невозможно, отсутствует ряд факторов: руководящая роль партии, моральный кодекс строителей коммунизма, Госплан и пр.
- Заимствовать рыночную НИС невозможно, поскольку также отсутствуют формирующие ее факторы (клубы, профессиональные сообщества, протестантская этика и пр.).

Следует отметить, что кризис имеет объективный характер. Он не связан с заговором элит, бюрократизмом или вороватостью русских чиновников. До тех пор, пока он не будет разрешен, наша «Силиконовая мечта» будет похожа на силиконовую куклу соответствующего назначения. Ни критика, ни уголовные дела, ни вера во всемогущество «оборонки» дело не поправят.

Пути выхода из кризиса

Современный русский поэт Тимур Зульфикаров написал о нашем времени такие строки: «Когда Россия идет на Запад – она попугай или обезьяна»*. Наверное, пора заканчивать «копировать передовой опыт» и начинать думать своей головой. В этом и есть путь выхода из кризиса.

В условиях неопределенности новую НИС можно только ВЫРАСТИТЬ. Так поступили наши отцы, создав советскую науку и технику. И у нас другого пути нет. Многолетнее копирование привело лишь к потере двух поколений творческой молодежи и девальвации потенциала советской науки и техники.

А для того, чтобы вырастить НИС, нужно использовать новые подходы, опирающиеся на иные принципы, которые могут быть воплощены в жизнь в реалиях современной России.

Нужно признать свою ответственность: за нас нашу мечту никто не воплотит. ИКС

* Т. Зульфикаров. «Идея России». Открытое письмо президенту Российской Федерации В.В. Путину. www.zulfikarov.ru/article9.

www.iks-consulting.ru

iKS CONSULTING

Энергия интеллекта

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

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

ИТ	Телеком	Медиа	Контент и сервисы
Системная интеграция	Голосовые услуги	Платное ТВ	Навигация и LBS
Дата-центры	ШПД	Мобильное видео	M2M
Облачные сервисы	Мобильный интернет	Игры	NFC
ИТ инфраструктура	VAS	Интернет-порталы	E-commerce
Офисная техника	Межоператорские услуги	Видеоконтент	Телемедицина

Реклама

Особенности создания облачного бренда

Николай Носов

При раскрутке облачного бренда лучше делать акцент на рациональные моменты, а не на эмоциональную вовлеченность. Важную роль играет использование нейтральных рекламных площадок – отраслевых конференций, изданий, сайтов, дающих разностороннюю информацию о брендах.

Реклама – двигатель торговли. Чтобы покупатель купил ваш товар, он должен про него узнать. Легко продать товар нужный и дефицитный. Вы платите за прямую рекламу, сообщаете, где и как можно купить, и регулируете очередь ценой. Но если рынок насыщен, то все становится сложнее. Мало сообщить, что продаете молоко. Этой информацией вы никого не привлечете. Надо, чтобы во время изучения бесконечного ассортимента условного «молока» в супермаркете у покупателя что-то щелкнуло в голове, возникла ассоциация с котом Матроскиным из Простоквашино, с давней мечтой купить «домик в деревне», или просто в памяти всплыло смутно знакомое название, и он бросил в тележку именно ваш пакет. Чтобы покупатель смог выделить продукт или сервис вашей фирмы из множества других, практически таких же товаров и услуг. Чтобы он знал ваш бренд и позитивно относился к нему.

Все это справедливо и для облачного рынка. Прошло время, когда кого-то можно было удивить предложением услуг IaaS. Да и другие облачные сервисы все чаще становятся типовыми. Основная масса игроков предлагает примерно одинаковый набор услуг, и для того чтобы покупатель остановился у вашего «прилавка», нужно вкладываться в бренд.

Бренд – это комплекс представлений, оценок, мнений, ассоциаций, эмоций, ценностных характеристик, связанный с продуктом либо услугой в сознании потребителя. Это именно то, что отличает товар или услугу компании от аналогичных предложений конкурентов.

Рис. 1. Топ-10 самых дорогих брендов в мире, 2019 г. ▼

Рейтинг	Бренд	Категория	Стоимость, $ млрд	Прирост к 2018 г., %	Страна
1	amazon	Ритейл	315,505	+ 52	
2		Технологии	309,527	+3	
3	Google	Технологии	309,000	+2	
4	Microsoft	Технологии	251,244	+25	
5	VISA	Платежи	177,918	+22	
6	facebook	Технологии	158,968	–2	
7	Alibaba.com	Ритейл	131,246	+16	
8	Tencent 腾讯	Технологии	130,862	–27	
9		Фастфуд	130,368	+3	
10	AT&T	Телеком	108,375	+2	

Источник: BrandZ

Самые узнаваемые

На мировом облачном рынке лидирует Amazon Web Services – подразделение компании Amazon, которая возглавляет список наиболее дорогих брендов рейтинга BrandZ Top 100 за 2019 г. (рис. 1). Не углубляясь в методику определения стоимости бренда, включающую оценку дисконтированных денежных потоков, которые генерирует бренд для предприятия, отметим, что в первой десятке только одна компания не ассоциируется с ИТ – это McDonald's.

Помимо Amazon в первой десятке еще два гиперскейлера: третье место занимает Google, четвертое – Microsoft. Неудивительно, что вместе этим трем компаниям принадлежит и 67% рынка публичных облаков (рис. 2).

Хорошо раскручен бренд у идущих следом Alibaba Cloud (бренд Alibaba Group – седьмой в

мировом рейтинге) и IBM Cloud (бренд IBM – 13-й). 47-ю позицию в BrandZ Top 100 занимает Huawei, 50-ю – Oracle.

Облачный бренд – представление об услуге на облачном рынке в головах его участников. Но для того чтобы в сознании сложилось представление о бренде, ему надо туда сначала попасть.

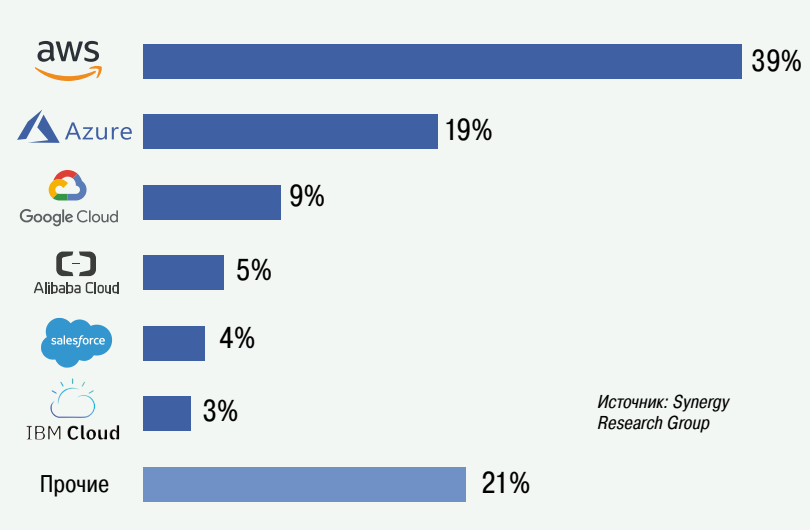
Продвижение на глобальном уровне не ведет автоматически к узнаванию облачного бренда на российском рынке. Проведенное в прошлом году iKS-Consulting исследование имиджей брендов облачных провайдеров показало, что наиболее узнаваемыми IaaS-брендами среди руководящих сотрудников компаний разных отраслей, причем с большим отрывом, являются бренды «Ростелеком» и КРОК. С «Ростелекомом» (компанию знали 63% респондентов) более или менее понятно – нацеленный на крупный бизнес российский телекоммуникационный гигант начал рекламировать свое облако «О7» (Национальную облачную платформу) еще в 2011 г. Второе место КРОКа (его знали 57% респондентов) – результат более неожиданный. Скорее всего, это следствие рекламной активности на протяжении всей долгой истории компании. Помнится, в далеком 1993 г. меня попросили купить очень дорогую, только появившуюся модель мультимедийного ноутбука. Смог найти компьютер лишь в тогда еще маленькой компании КРОК, занимавшей небольшое помещение в районе Садового кольца. С той поры компания сохранила имидж фирмы, торгующей дорогой высококачественной продукцией, который смогла перенести в область интеграции, а затем и в облака. Хотя сегодня компания воспринимается больше как системный интегратор, а не как облачный провайдер.

Единственной хорошо узнаваемой в нашей стране облачной компанией из лидирующих на международном уровне оказалась Microsoft, которая активно работает и в России. Этот факт еще раз подтверждает, что компаниям необходимо рекламировать свои глобальные бренды на локальных рынках и присутствовать в информационном поле интересующих их стран.

Под зонтиком старого бренда

Запуск новых сервисов под зонтиком существующего бренда – обычная практика на рынке. Из лидирующих на мировом рынке облаков компаний только предлагающая PaaS- и SaaS-сервисы Salesforce не имеет бренда, входящего в BrandZ Top 100. Остальные успешно используют ранее созданный бренд.

Самым дорогим российским брендом третий год подряд признается Сбербанк (рис. 3). Его стоимость в 2019 г. была оценена аналитиками компании Brand Finance в 842,1 млрд руб. Это на



▲ Рис. 2. Доли облачных провайдеров на мировом рынке публичных IaaS- и PaaS-сервисов

25,6% больше, чем годом ранее. Неудивительно, что этот бренд пытаются использовать на облачном рынке. Сначала Сбербанк собирался развивать облачную платформу SberCloud совместно с компанией «Сервионика» (ГК «Ай-Теко»), затем решил заняться платформой самостоятельно, а общее детище под брендом «СБКлауд» продолжает растить «Ай-Теко». Путаница в названиях вряд ли идет на пользу обоим брендам, во всяком случае сейчас эти платформы путают даже специалисты, но наличие отсылки к Сбербанку бесспорно добавляет им узнаваемости.

Сбербанк активно предоставляет свой бренд для самых разных услуг. Если бизнес связан с финансами, то использование известного бренда может быть полезным. Я сам один раз стра-

Рис. 3. Топ-10 самых дорогих брендов России, 2019 г. ▼

Рейтинг	Бренд	Стоимость, млрд руб.	Прирост к 2018 г., %
1	СБЕРБАНК	842,1	+ 25,6
2	GAZPROM	552,2	+ 72,1
3	ЛУКОЙЛ	397,2	+41,3
4	РОСНЕФТЬ	246,9	+21,1
5	РЖД	185,8	+16,9
6	МАГНИТ	170,3	+17,4
7	ВТБ	144,8	+23,3
8	TATNEFT	132,4	+36,2
9	МТС	121,5	+6,1
10	НОВАТЭК	119,9	+59,1

Источник: Brand Finance

Антон Салов, независимый эксперт RCCPA

Облачный бренд проще формировать в уже существующей компании. На его восприятие будут влиять опыт и профиль компании, так что нужна правдивая история о том, как ДНК основного бизнеса связана с облачным направлением, как преимущества существующего бизнеса помогают созданию нового.

Другая важная часть облачного бренда – люди, которые стоят за проектом. Важно, чтобы они имели хорошую репутацию, открытую позицию и были готовы взаимодействовать с облачным сообществом.

ховался для поездки за рубеж через «Сбербанк-страхование». С одной стороны, это оказалось намного дешевле, чем у лидеров рынка, с другой – итоговый договор заключался не со Сбербанком, а с совершенно неизвестной компанией, не вызывавшей никакого доверия. И ответственность по договору несла она. Так что в конце концов вернулся к более дорогим, но проверенным брендам.

В случае облаков роль будет играть не столько известная надежность финансового учреждения, сколько имидж «самой большой ИТ-компании с банковской лицензией». На компании с большой долей государственного участия положительное влияние окажут вовлеченность Сбербанка в программу «Цифровая экономика России» и ассоциации с государством.

Девятое место в рейтинге самых дорогих брендов России занимает МТС – 121,5 млрд руб., рост за год 6,1% (см. рис. 3). Телеком больше ассоциируется с облаками, так что бренд #CloudMTS выглядит перспективно. Сейчас его уже узнают на нашем рынке. Как будут дальше развиваться эти облачные бренды – покажет время.

«Скелеты» старого бренда

«Зонтик» старого бренда может переносить на облака и негативный опыт клиента. Так, несмотря на все усилия нынешнего CEO Microsoft Сатьи Наделлы, разворачивающего бизнес компании в облака, она по-прежнему ассоциируется в основном с десктопной операционной системой. В памяти всплывают отголоски информационных войн глобального уровня – слоган Microsoft must die, «синий экран смерти». Негативный опыт смены Windows 3.1 на Windows 95 и Windows XP на Windows Vista заставляет с осторожностью подходить к смене версий ОС. И прекращение поддержки Windows 7 ставит пользователя перед непростым выбором, что тоже не улучшает восприятие компании.

По облачному бренду Microsoft Azure ударило и громкое дело, связанное с первоначальным отказом и последующей передачей правительству США данных из облака провайдера в Ирландии. Принятый властями США «облачный» закон (CLOUD Act) позволяет правоохранительным органам получать от американских ИТ-компаний хранящиеся у них данные граждан США, в том числе находящиеся за рубежом. Разоблачения Сноудена заставляют задуматься граждан и других стран. Война санкций и политика импортозамещения уменьшают перспективы использования облаков американской компании в российских госструктурах. Правда, эти факторы не всегда критичны для отечественных компаний, стремящихся к выходу на глобальные рынки.

Активно ведет себя на российском облачном рынке компания Huawei. Позитивные впечатления от использования популярных в России смартфонов компании переносятся и на облачные сервисы, хотя про них знают еще немногие. С геополитической точки зрения китайский гигант находится на нашем рынке в более комфортной ситуации, чем Microsoft. Китай рассматривается как союзник, и зачастую импортозамещение сводится к замене американских продуктов китайскими, особенно при отсутствии российских товаров и сервисов аналогичного качества. Так что облачные сервисы компании могут найти применение в российских госструктурах и компаниях, контролируемых государством.

Но китайское происхождение компании вызывает и негативные ассоциации, влияющие на бренд. Здесь сказываются и опыт использования быстро ломающейся продукции неизвестных китайских производителей («китайское – значит ненадежное»), и информационная война, которая ведется против китайских ИТ-компаний на Западе («китайские компьютеры шпионят за пользователями»). Широко освещавшиеся в СМИ американские санкции против Huawei влияют на оценку рисков работы с облачными сервисами компании, но, с другой стороны, могут улучшать эмоциональное восприятие бренда («обижают, как и российские компании»).

Даже положительный образ бренда-зонтика может негативно влиять на создаваемый под ним облачный бренд. Бренды «Яндекс» и Google вызывают стойкие ассоциации с поисковой системой, Mail.ru – с почтовым сервисом. Компаниям «Яндекс» и Mail.ru отчасти удалось перенести «зонтичную» популярность на свои об-

лачные бренды. Положительную роль сыграли сервисы «Яндекс.Облако» и «Облако Mail.ru». Когда у меня спрашивали «Что такое облако?» люди, далекие от компьютерных технологий, то приводил в пример эти сервисы. Сразу становилось понятно: облако – это средство хранить фото где-то далеко, а не на своем смартфоне. А вот никак не проявляющая себя в российском информационном поле Google по-прежнему воспринимается как поисковик, а то, что это один из ведущих игроков мирового облачного рынка, в том числе и IaaS, знают только специалисты.

Похожая ситуация и с компанией Oracle, которая воспринимается как поставщик «очень надежной и очень дорогой СУБД». Десять дет назад Ларри Эллисон заявлял, что «облачные вычисления – это бред сивой кобылы». Спустя три года эксцентричный миллиардер уже сравнивал переход к облачным вычислениям с компьютерной революцией и пытался ее возглавить. Отчасти задача была решена – компания стала одним из лидеров на рынке облачных вычислений. Но в России облачный бренд практически незаметен, и компания по-прежнему ассоциируется со своим флагманским продуктом – СУБД.

В отличие от лидирующей в мире AWS компания Oracle имеет представительство в России и активно работает с российским рынком. Для раскрутки облачного бренда используется рациональный подход – «теория гравитации данных». Обрабатывать данные быстрее в месте их сбора или хранения, поэтому проще перенести вычислительные мощности к данным, чем гонять запросы по сети. Как звезды за счет гравитации притягивают к себе небесные тела, так и данные притягивают к себе обрабатывающие их приложения. Наиболее популярна на рынке СУБД Oracle, «центры притяжения» находятся как в базе данных облака Oracle, так и на площадке клиента, так что логичным представляется использование облачных сервисов Oracle, «притянутых» к данным.

Для большей «привязки» компания активно развивает интеграционную платформу iPaaS, позволяющую интегрировать популярные у разработчиков open source-решения между собой и самое главное – с базой данных Oracle. Так за счет популярности базы данных продвигаются облачные сервисы, прежде всего PaaS. Из облака предлагаются средства организации разработки, контейнеры, системы искусственного интеллекта и даже блокчейн. В российских условиях акцент делается на том, что данные остаются на площадке заказчика, а облачные сервисы предлагаются разработчикам как глубоко интегрированные с СУБД Oracle.

Лояльность к облачному бренду

В рамках исследования iKS-Consulting компанию Microsoft назвали облачным провайдером только 26% пользователей IaaS. При этом она возглавила рейтинг лояльности IaaS-провайдеров в России. Респонденты, поставившие компании наивысший балл, отмечали эмоциональное восприятие бренда, а именно: «Это всемирно известная компания, надежная, ей все доверяют», «Успешная компания с хорошей историей», «Большой и матерый игрок. Все ошибаются, но у них это реже» и т.п. Так что действующие пользователи компанией в целом довольны.

С расширением клиентской базы стоимость привлечения нового клиента к одной и той же услуге начинает увеличиваться. Обострение конкуренции на облачном рынке, выдавливание мелких игроков требуют от компаний работы с брендом. Прежде всего стоит вкладываться во внутренний бренд, работу с сотрудниками и существующими клиентами. Лучшую конверсию (3,63% по оценкам iKS-Consulting) дает канал «клиент по рекомендации», который возникает в процессе работы с внутренним брендом, накопления опыта работы с компанией. Нужно, чтобы клиент знал, как зовут его персонального менеджера, нужно разрабатывать стандарты и обучать людей, предоставляющих сервис поддержки. Изменить уже сформировавшееся мнение аудитории, особенно то, которое сложилось на основе личного опыта, очень трудно.

Дмитрий Горкавенко, директор по развитию бизнеса, iKS-Consulting

Результат говорит о хорошем умении Microsoft работать с существующими клиентами, в терминологии некоторых экспертов – с внутренним брендом. Внешний бренд – то, как воспринимают компанию бизнес, население, СМИ, – тоже важен, но экономически выгоднее удерживать имеющихся клиентов, чем привлекать новых, да и лучшим способом привлечения новых клиентов являются рекомендации существующих.

Хороший сервис в глазах клиента часто важнее цены. Время клиента – тоже деньги, которые экономит быстрое и качественное обслуживание. Важен опыт взаимодействия с об-

лачным провайдером, работы в нештатных ситуациях. Аварии бывают у всех, никто не застрахован от удара молнии, пожара, обрыва кабеля экскаваторщиком. Но реагируют на аварии по-разному.

Хороший пример – реакция компании DataLine на пожар на крыше ее ЦОДа в Москве в июне 2019 г. Провайдер оперативно информировал клиентов о событии, о принятых мерах, рассказывал о ситуации на своем сайте и даже выкладывал изображения ситуационных экранов по залам с температурами холодных коридоров. Задержки в предоставлении облачных сервисов были, но в целом имидж компании не пострадал. А проверка инженерных систем, герметичности гермозон (на крышу при тушении пожара вылили много воды) и четкое выполнение регламентов аварийных работ в боевых условиях скорее даже положительно сказались на бренде.

«Особенность раскрутки облачного бренда – ориентация на рациональные моменты, а не на эмоциональную вовлеченность», – отметил директор по развитию бизнеса iKS-Consulting Дмитрий Горкавенко. А рациональный выбор осуществляется не только по техническим характеристикам сервиса и анализу SLA, но и исходя из опыта работы в аварийных ситуациях.

Рис. 4.
Этапы создания бренда ▼

Этапы создания бренда

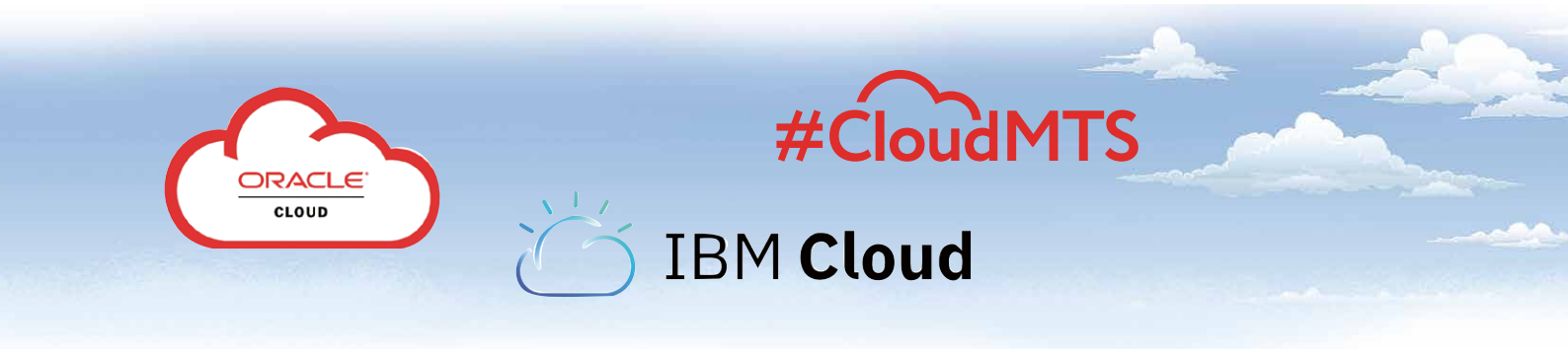
Основными этапами создания облачного бренда являются разработка стратегии и позиционирование бренда; нейминг; разработка фирменного стиля (визуализация); разработка паспорта стандартов бренда и руководства по фирменному стилю; внедрение бренда, его сопровождение и аудит (рис. 4).

Наиболее важен первый этап, на котором проводятся маркетинговые исследования, позиционирование бренда, разрабатывается стратегия продвижения. Облачный бренд должен выделиться не только за счет психологической составляющей, но и за счет правильного позиционирования на рынке. Например, «Ростелеком» воспринимается как крупный игрок для государственных структур – именно они прежде всего обратят внимание на компанию при выборе облачного провайдера. КРОК – провайдер для работы с частными облаками. Благодаря активной рекламе Kubernetes as a Service компания Mail.ru воспринимается на российском облачном рынке едва ли не как синоним Kubernetes, а ее бренд ассоциируется с рынком PaaS. Есть компании, ориентированные на узкие профессиональные ниши, – например, облако ЦФТ в Новосибирске создано для предоставления банковских услуг (интернет-банк Faktura.ru, автоматизированная банковская система). Это облако представляет интерес для банков, использующих ПО компании.

На втором этапе разрабатывается название бренда (нейминг). Название должно быть простым и легко запоминающимся. Как шутят маркетологи, плох тот специалист, который не может придумать название бренда из трех букв. Вспомним AWS, IBM, МТС. В крайнем случае – не более трех слогов: Microsoft, Google, Huawei.

Для облачных провайдеров характерно использование в названии слов «облако» или cloud: «Яндекс.Облако», Mail.ru Cloud Solutions, #CloudMTS, Cloud4Y. Это помогает плохо разбирающемуся в рынке клиенту идентифицировать компанию как облачную. Той же цели служит третий этап – разработка логотипа компании, который часто включает изображение облака. Подобные логотипы есть почти у всех облачных провайдеров, входящих в BrandZ Top 100 (рис. 5).

Минимальный набор носителей бренда – название, логотип и цвет. Но часто используются расширенные наборы, включающие слоган (например, «Think!» компании IBM); легенду бренда; брендбук; фирменную документацию (визитки, конверты, папки, бланки, ежедневники); рекламную полиграфию (баннеры, буклеты, каталоги, листовки, упаковки); фирменный персонаж (например, крокодил у КРОКа и зеленый



▲ **Рис. 5. Логотипы наиболее популярных облачных брендов**

дракончик у Selectel); фирменную одежду и оформление транспорта; сувенирную продукцию (ручки, зонты, зажигалки, блокноты, футболки); средовой дизайн (фирменный стиль в интерьере офиса, выставочные или рекламные стенды), цифровые носители (сайт, электронные презентации, мобильные приложения); фирменную мелодию.

Четвертый этап – разработка паспорта стандартов бренда и руководства по фирменному стилю. Следует документально зафиксировать положения о концепции бренда, его целях, описать особенности каждого носителя фирменного стиля, создать для него технический документ.

Завершающий этап брендинга – внедрение, сопровождение и аудит – самый дорогостоящий. Нужно обучить персонал правильному взаимодействию с клиентами. Изготовить упаковку, печатную продукцию, вывески, разработать сайт, провести рекламную кампанию и контролировать выполнение требований, сформулированных в стратегии бренда. Причем процесс этот непрерывный – сайт должен обновляться, персонал контролироваться, реклама периодически появляться в СМИ.

Рекламные кампании

Согласно исследованию iKS-Consulting, 71% клиентов узнает об облачном бренде через отраслевые мероприятия. Для поддержания внутреннего бренда облачные компании проводят свои отраслевые мероприятия, где имеют максимально комфортные условия для рекламы. В памяти всплывают российские конференции Microsoft, Huawei, IBM, Oracle. Проводят свои конференции и российские облачные провайдеры – «Яндекс» (конференция Yandex Scale), Mail.ru (mailto:CLOUD), Selectel (SelectelTechDay). На таких мероприятиях воздействие осуществляется как на психологическом уровне (оформление зала, подарки, атмосфера), так и на рациональном – объясняются преимущества решений компании.

Грамотно выстроена рекламная кампания предоставляющей услуги colocation IXcellerate, которая воспринимается как нейтральный дата-центр мирового уровня для локализации зарубежных облаков. На проводимых компанией мероприятиях постоянно подчеркивается ее интернациональность («мир как большая деревня» на фестивале Rockin'Russia 2019), английское качество (визит принца Майкла Кентского на открытие нового дата-центра в Москве, концерт шотландских волынщиков). Позитивно играют на бренд нестандартные новогодние подарки клиентам – плюшевые тигрята, деньги за которые пошли в WWF на поддержку работы с конфликтными амурскими тиграми.

Хорошо влияет на психологическое восприятие бренда наличие экологических программ. Международные компании поддерживают внешний бренд и за счет участия в решении глобальных проблем. Например, Microsoft недавно анонсировала, что к 2030 г. достигнет отрицательного уровня углеродных выбросов. Сотрудникам не запретят выдыхать углекислый газ – цели планируется добиться благодаря переходу на электромобили и высадке лесов.

Конференции вендоров способствуют улучшению восприятия бренда у уже имеющихся клиентов, но не столь эффективны для привлечения новых. Для рационального воздействия больше подходят нейтральные площадки, где потенциальные клиенты могут сравнить решения разных поставщиков, в кулуарах обменяться опытом работы с ними и сделать осознанный выбор. У облачников наиболее популярна конференция Cloud & Digital Transformation, проводимая «ИКС-Медиа». Среди других площадок стоит отметить облачную секцию CNews Forum и облачную конференцию TAdviser. В последнее время заметную роль в обмене мнениями о работе облачных сервисов стали играть соцсети, например группа RCCPA в Facebook. Оперативное реагирование на критику в соцсетях также способствует усилению облачного бренда.

...Поддержание бренда подобно езде на велосипеде: надо все время крутить педали. Конкуренты не дремлют. Прекращение финансирования продвижения бренда быстро приведет к его ослаблению, так что пиар-службы игроков облачного рынка без работы не останутся. ИКС

Пионеры ЦОДостроения
Московская биржа

Александр Барсков

Московская биржа уже более 25 лет успешно развивает систему центров обработки данных, используя как собственную площадку, так и коммерческие дата-центры. История развития ее ИТ-площадок отражает основные этапы становления российской отрасли ЦОДов.

Московская биржа, тогда Московская межбанковская валютная биржа (ММВБ), была учреждена в январе 1992 г. Поначалу торги валютой проходили в «ручном» режиме, а компьютеры применялись лишь для ведения протоколов, по сути, как пишущие машинки.

«Ты помнишь, как все начиналось…»

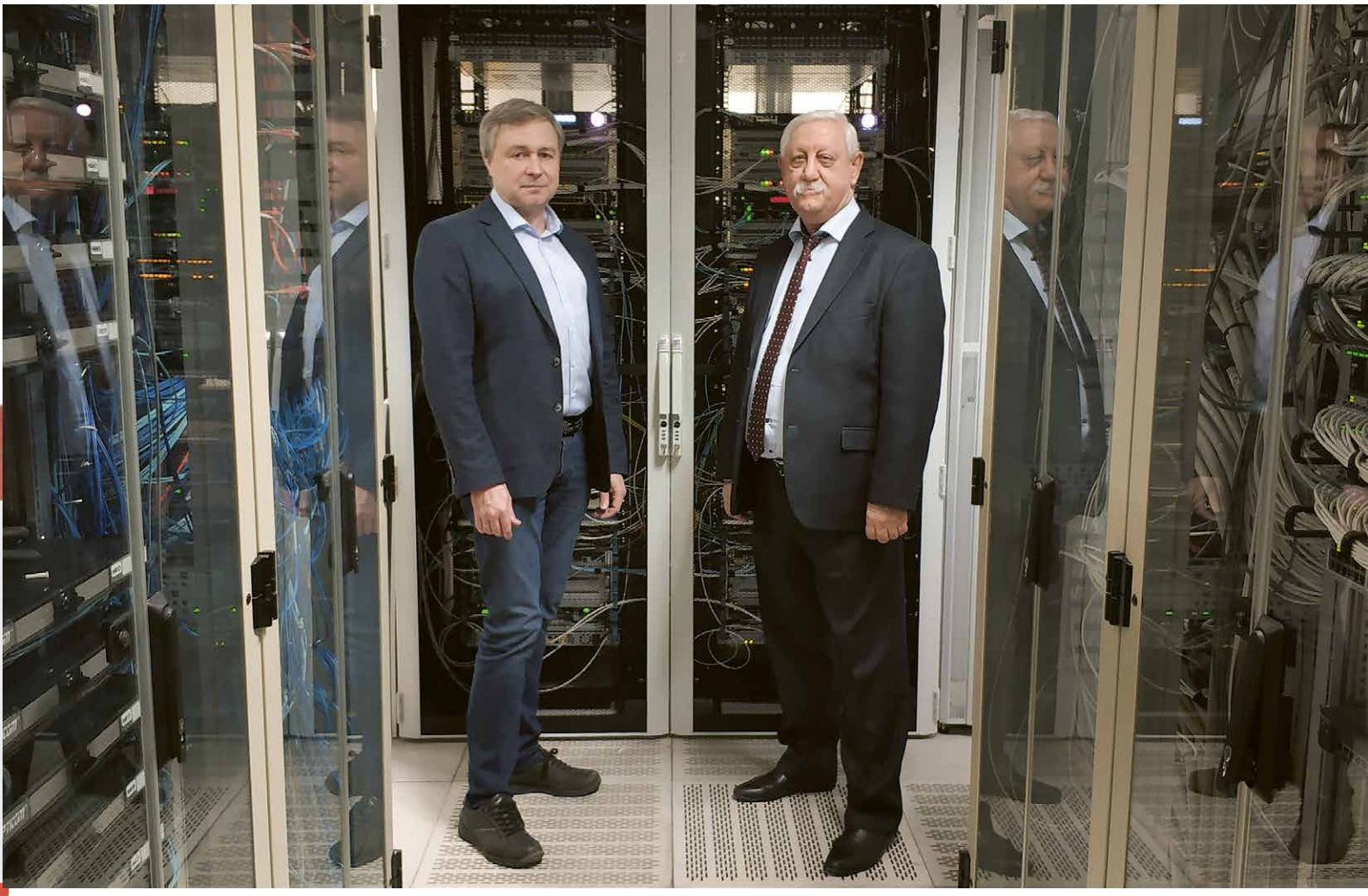
Большой электронный проект на бирже стартовал в начале 1993 г. в связи с необходимостью обеспечить проведение аукционов и торгов по ГКО – государственным краткосрочным бескупонным облигациям. Для организации первого вычислительного центра (термина «дата-центр» тогда еще не существовало) было выбрано здание «РИА Новости» на Зубовском бульваре. В этом здании, построенном в расчете на Олимпиаду-80, был стандартный по меркам конца 70-х годов прошлого века вычислительный центр.

«Мы сняли сначала одно помещение, потом рядом – второе. Начинали с четырех RISC-машин – двух больших серверов (HP 9000/890 Emerald), двух малых (HP H20) и рабочей станции. В том же помещении установили ИБП», – вспоминает Сергей Мещерин, ныне директор по информационным технологиям Московской биржи. – Электричество брали от существующего ВЦ. Как была устроена система электроснабжения с внешней стороны, мы не знали, но считалось, что ВЦ «РИА Новости» запитан правильно».

На биржу пришли специалисты главным образом из ВПК, с большим опытом в области промышленных технологий обработки данных. Они постарались реализовать все лучшие наработки в сфере обеспечения надежности и построения отказоустойчивых систем.

Резервировать инженерные системы стали сразу. Использовали два ввода электропитания (правда, оба от ВЦ «РИА Новости»), ИБП тоже установили два (2N). Система кондиционирования, хоть и строилась на бытовых «сплитах», но была резервирована по схеме 3N: в помещении стояли три кондиционера, а для нормальной работы хватало одного. Был организован контур безопасности (дополнительные двери, СКУД), чтобы в комнаты с ИТ-оборудованием биржи не проник посторонний. Все было сделано просто, но надежно.

2020 год.
ЦОД Московской биржи в Кисловском переулке. Слева – Сергей Кобзев, начальник управления развития и эксплуатации ЦОД Московской биржи, справа – Сергей Мещерин, директор по ИТ Московской биржи ▼



▲ 1997 год.
В ЦОДе Московской биржи, расположенном в высотном здании в районе станции метро «Красные Ворота»

Второй ЦОД

В 1995 г. ММВБ стала активно развивать удаленную инфраструктуру, сначала в Москве, а потом и в регионах России. На рубеже 1996 г., когда формирование региональных структур было, по сути, завершено, большая часть пользователей подключалась к ИТ-системе удаленно.

К тому моменту вполне созрело понимание того, что для повышения надежности системы торгов, как, впрочем, и иных систем обработки данных биржи, необходимо удаленное резервирование вычислительной среды, понемногу сложилась модель двух вычислительных центров, дублирующих друг друга. Руководство организации поддержало эту идею и приняло решение о создании второй ИТ-площадки. У биржи был офис в высотном здании в районе станции метро «Красные Ворота», в нем-то, на 12-м этаже, и было решено создать второй вычислительный центр.

К этому времени появился собственный опыт эксплуатации объекта, стали очевидными пути его совершенствования. Все они лежали в области использования промышленных подходов. При проектировании большое внимание было уделено организации системы гарантированного и бесперебойного электропитания. Для нового ВЦ были задействованы два ввода из города: один от трансформаторной подстанции, обслуживающей метрополитен, другой – от подстанции троллейбусной сети. Такие ТП считаются весьма надежными. Кроме того, для нового ВЦ был установлен дизель-генератор – его разместили в гараже под зданием и организовали специальный выхлоп. Для ИБП и батарей выделили специальные отдельные комнаты, откуда гарантированное бесперебойное электропитание подавалось в машинный зал.

Сам зал был небольшим – около 60 кв. м. В отличие от ВЦ на Зубовском, на новом объекте уже была установлена промышленная система кондиционирования – с резервированием 2N. Выгораживать холодные коридоры не требовалось, поскольку кондиционер отлично охлаждал все помещение. Также система кондиционирования охватывала помещения ИБП. На объекте были реализованы промышленные системы противопожарной сигнализации, автоматического газового пожаротушения, безопасности, видеонаблюдения – все как делается сегодня, в современных ЦОДах. Заметим – шла середина 90-х годов...

Новый объект запустили в эксплуатацию в 1997 г. Некоторое время он рассматривался в качестве резервного. После того, как специалисты биржи убедились в надежности новой площадки, ВЦ на Красных Воротах стал основным, а на Зубовском – получил статус резервного. Торговая система использовала главный сервер (engine) и серверы доступа (gateway). Серверы доступа стояли как в основном, так и в резервном ВЦ. Они работали постоянно, но подключались только к главному серверу, размещенному в основном ВЦ. Второй главный сервер находился в «холодном» резерве.

В дополнение к торговому залу на Зубовском в здании на Красных Воротах развернули еще два зала. Проблем с удаленной работой не возникало, поскольку задержка в каналах связи не имела в то время большого значения – трейдеры набирали данные на клавиатуре, а скорость набора была существенно ниже скорости обработки запросов.

В какой-то момент специалисты биржи поняли, что для надежной связи между площадками мало обычных каналов связи – нужна своя оптика. Проблемы были не в пропускной способности используемых каналов, а в их надежности. Телекоммуникации тогда только развивались, поэтому надежность каналов, арендуемых у провайдеров, оставляла желать лучшего. Появилась идея – проложить «темное» оптоволокно между двумя вычислительными центрами для обеспечения их надежной связи друг с другом. Однако реализовать ее удалось позднее, в рамках строительства следующего объекта. Впоследствии для всех новых объектов биржи (не только ЦОДов, но и офисных зданий) стали сразу прокладывать свою оптику, экспериментируя при этом с моделью владения – собственная линия или аренда. Как считают специалисты биржи, этот подход многократно оправдал вложенные в него средства, много раз выручал в процессе развития и совершенствования промышленных технологий обработки данных организации.

ЦОД в своем здании

Биржа активно развивалась, открывались новые рынки, совершенствовались технологии

торгов и расчетов, появлялись иные виды обслуживания, повышались требования к его качеству. Со временем ВЦ на Зубовском перестал удовлетворять возросшим потребностям. Было принято решение постепенно от него отказаться. Опять встала задача поиска второй площадки, так как было понятно, что модель двух ЦОДов является ключевой для обеспечения требуемой надежности.

Во второй половине 90-х биржа приобрела комплекс зданий в Большом Кисловском переулке, и именно там началось строительство нового ЦОДа. Капитальный ремонт здания проводился уже с учетом того, что на одном из этажей будет размещаться ИТ-комплекс. Были сделаны более вместительные вертикальные шахты, больше места было выделено под воздуховоды.

«Здесь, в новом здании, все старались делать капитально, с возможностью дальнейшей модернизации. ИБП, батареи и дизель разместили в специальных помещениях в подвале. Максимально грамотно сделали выхлоп, учтя некоторые ошибки, допущенные при создании ВЦ на Красных Воротах. Все магистрали заранее спланировали и проложили. А со временем, как и положено, выделили и оборудовали холодные коридоры в машинном зале», – рассказывает С. Мещерин.

Новый ЦОД с машинным залом площадью 192 кв. м был запущен в эксплуатацию в конце 1999 г. В него были переведены системы с Зубовского бульвара. Поначалу ЦОД казался полупустым – в машзале стояло менее десятка стоек с ИТ-оборудованием.

«Мы построили ЦОД с большим запасом. И это не раз нас выручало. Сегодня в том же помещении, с той же инженерной инфраструктурой размещаются уже 65 стоек, и всё хорошо работает. Например, чиллеры, которые ставили с помощью вертолетов на крышу, служат нам до сих пор. Работает и установленный в подвале динамический ИБП с дизелем», – рассказывает Сергей Кобзев, начальник управления развития и эксплуатации ЦОД Московской биржи.

Следует отметить, что в ЦОДе в Большом Кисловском переулке был обеспечен очень высокий уровень надежности. Например, для системы бесперебойного питания была реализована схема 4N. «В интересах ЦОДа использовались две пары статических ИБП. Можно было работать при выходе из строя трех ИБП из четырех и проводить регламентные работы без отключения электропитания оборудования. Система ИБП для питания офиса строилась отдельно. Более того, напряжение на вход статических ИБП поступало с маховика динамического ИБП. Постепенно мы ушли от такой сложной схемы резервирования, отдав предпочтение классической схеме 2N», – делится опытом С. Кобзев.

Потребность в серверах стремительно росла, и новый ЦОД стал быстро заполняться. В машинный зал устанавливали все новые и новые системы, в том числе и те, которые изначально являлись офисными и не были критически важными для работы биржи. Так, внутренняя почта дала толчок к созданию системы электронного документооборота. Значимость этой системы существенно выше, чем обычной почты. Ей понадобились резервные серверы и надежная инфраструктура ЦОДа. И таких систем становилось все больше.

Быстро развивалась и телекоммуникационная составляющая как самого ЦОДа, так и организации в целом. Сначала биржа использовала услуги всего двух провайдеров телекоммуникационных услуг: основного и резервного. Но затем клиенты попросили увеличить число провайдеров, поскольку на их объектах присутствовали свои операторы связи – в то время чужих провайдеров в здания, как правило, не пускали. С ростом числа провайдеров и расширением сети биржи в ЦОДе росло и число телекоммуникационных стоек.

Что касается статуса нового ЦОДа, то здесь повторилась история с площадкой на Красных Воротах: в какой-то момент он поменялся с резервного на основной. В такой конфигурации биржа «жила» до 2007 г. Тогда владельцам здания на Красных Воротах потребовались помещения, занимаемые биржей, и они попросили съехать. Опять возникла задача поиска резервного ЦОДа...

В поисках КЦОДа

К тому моменту в России стали появляться коммерческие ЦОДы. «Мы увидели, что рождается совершенно новое направление обслуживания клиентов – предоставление места в коммерческом ЦОДе в качестве услуги. Некая ор-

2001 год.
В серверном зале ЦОДа Московской биржи в Кисловском переулке ▼

ганизация строит ЦОД, а потом сдает его ресурсы другим компаниям. Сначала это выглядело странно, доверие – нулевое. Что у них там, как сделано? Кабели, ИБП, кондиционеры еще можно увидеть. А как организована служба эксплуатации и поддержки как самого объекта, так и пользователей?», – перечисляет опасения С. Мещерин.

Перед биржей встал важный вопрос: строить самим или арендовать. «И сейчас мы от этого вопроса не ушли. Он периодически поднимается, просчитываются варианты. Понимаем, что строить самим – хлопотно и дорого. Да и считать можно по-разному. Если брать пятилетнюю модель – одна экономика, десять лет – совсем другая. Все зависит от горизонта планирования. Мы стараемся бережно относиться к нашим финансовым ресурсам, поэтому раз за разом просчитываем возможные варианты», – продолжает директор по ИТ Московской биржи.

Тогда, в середине 2000-х, на строительство своего ЦОДа времени просто не было. Жизнь заставила идти в коммерческий ЦОД, и этот вариант впоследствии себя оправдал. В то время выбор был небольшой – две-три площадки. Была выбрана самая на тот момент новая – ЦОД «Стек Телеком» на площадке М1. По сути, этот провайдер оказался единственным, кто смог предоставить сервис нужного качества и объема (порядка 40 стоек).

Как вспоминают на бирже, переезду предшествовали серьезные работы по совершенствованию провайдером своей площадки, отработке регламентных процедур. «У нас коэффициент доступности основных систем – 99,97, значит, ЦОД должен иметь соответствующий показатель – минимум 99,99. Мы пришли к провайдеру услуг ЦОДа с такими требованиями и дополнительными пожеланиями по обеспечению физической безопасности. Изначально у него не было опыта предоставления сервиса подобного уровня доступности. Компания с энтузиазмом подошла к выполнению наших весьма жестких требований, они сами многому научились, внедрили в практику своей деятельности некоторые принципиально новые инженерные и организационные подходы. Это была совместная сложная, но интересная работа, которая дала весомые плоды обеим организациям», – говорит С. Мещерин.

В сентябре 2007 г. биржа «встала» в коммерческий ЦОД «Стек Телеком». Между М1 и ЦОДом в Большом Кисловском переулке сразу была проложена «темная» оптика в виде кольца, реализовано «горячее» резервирование. Сначала площадку на М1 использовали как резервный ЦОД. Впоследствии история повторилась в третий раз: новая площадка стала основной. «Впрочем, в нашем случае понятия "основной" и "резервный ЦОД" немного условны. Для одних систем основные серверы стояли на М1, резервные – в Кисловском. Для других – наоборот», – отмечает С. Кобзев.

Третья площадка

Число единиц серверного оборудования, используемого биржей, подскочило при переходе с RISC-машин на серверы x86. «В какой-то степени нас «подвела» ИТ-индустрия. Мы начинали с RISC-серверов, больших мощных надежных машин. Но рынок потребовал перехода на принципы высокочастотного трейдинга (High-Frequency Trading, HFT), а это, в свою очередь, заставило намного увеличить скорость обработки данных. Оказалось, что RISC-серверы просто «не тянут». Их операционные системы работали медленно. Мы вынуждены были с UNIX перейти на Linux, а с RISC-машин – на обычные серверы x86. Поначалу переход с точки зрения утилизации ресурсов ЦОДа нам казался простым. Но при использовании серверов x86 резко увеличилось их количество, число сетевых соединений, потребовались дополнительные средства обеспечения безопасности и мониторинга, и, как следствие, выросла потребность в стоечном пространстве, усложнилась модель использования ЦОДа. Количество перешло в качество», – продолжает С. Мещерин.

В 2011 г. состоялось объединение двух крупнейших российских бирж – ММВБ и РТС. Единая структура получила название «Московская биржа». Встала задача интегрировать ИТ-системы организаций, а для этого надо было перевести ИТ-ресурсы РТС с ее площадок в общие ЦОДы. Сначала их переместили в ЦОД в Большом Кисловском переулке. Но вскоре стало понятно, что емкости двух имеющихся площадок уже не хватает. Необходимо было искать третью.

К тому времени доверие к коммерческим ЦОДам выросло, на рынке появились новые серьезные игроки. Поэтому новую площадку искали на базе одного из коммерческих датацентров. А поскольку выросли и требования регулятора к качеству организации торгов, и требования клиентов к уровню обслуживания, главным критерием стала максимальная надежность. В тот момент в Москве появилась первая площадка, которая строилась строго по стандартам, – DataSpace.

«Этот объект мы вели долго. Ведь строился первый в России ЦОД Tier III. Конечно, с технической точки зрения разместить свои ресурсы в таком ЦОДе было весьма привлекательно. Строился он по всем правилам. Все думали, сделают или нет. Сделали! Ну и формальности были соблюдены – ЦОД первым получил все три сертификата

Uptime Institute», – говорит С. Мещерин. Вопрос выбора площадки обсуждался на всех уровнях руководства биржи, оценивались все за и против. Выбор был сделан в пользу DataSpace.

ЦОД биржи на площадке DataSpace был запущен в эксплуатацию в 2015 г. В нем два зала по 72 стойки: один зал биржа использует для своих нужд, второй – для размещения оборудования клиентов. «Мы видели много разных объектов. Считаем, что наш зал образцовый. Была возможность все сделать правильно, и мы ее не упустили, – вспоминает С. Кобзев. – С площадкой М1 так красиво не получилось. Заезжали с одним оборудованием, потом устанавливали другое. Технологии развивались, менялись, пришлось заменить стойки, выгородку, трудно было изначально заложить правильные коридоры».

Когда важна задержка

В конце нулевых годов ужесточились требования к задержкам при работе с торговыми системами биржи. Связано это было с развитием высокочастотного трейдинга, который сегодня является основной формой алгоритмической торговли на финансовых рынках. Когда торговали люди, компьютер трейдера мог располагаться где угодно, задержка не имела большого значения. В HFT используются специальные торговые стратегии и алгоритмы, при работе которых величина задержки критически важна. Когда появилась HFT-торговля, особо умные трейдеры стали размещать свои серверы максимально близко к серверам торговой системы. Началось это в те времена, когда главный сервер торговой системы находился на М1. Трейдеры вставали в разных залах ЦОДа М1, поэтому условия доступа могли быть неравными, а обеспечение равных условий доступа – одна из основных обязанностей биржи. Чтобы уравнять условия, специалистам биржи пришлось применять определенные технические решения. В дальнейшем в рамках площадки М1 появился зал colocation, где устанавливали свое оборудование клиенты биржи, работающие в модели HFT. После перевода главного сервера в ЦОД DataSpace специалистам биржи стало проще решать эту задачу. Специальный зал с серверами клиентов расположен рядом с машинным залом самой биржи, и у всех одинаковые возможности – разница в несколько метров не играет большой роли.

Необходимость обеспечить равные условия доступа не позволила бирже реализовать модель единого вычислительного пространства, когда неважно, в каком ЦОДе запущена основная система. «Для торговой системы трудно обеспечить равные условия доступа с точки зрения задержек – счет идет на микросекунды. Если бы не эта специфическая черта, мы бы реализовали такую модель, которая является более гибкой, дает больше простора для маневрирования вычислительными ресурсами, в особенности в нештатных ситуациях, – полагает С. Мещерин. – Сегодня зона колокации с оборудованием трейдеров размещена только в основном ЦОДе. Наверное, этот факт можно считать определенным недостатком нынешней инфраструктуры биржи, но строить зал колокации в резервном ЦОДе – удовольствие дорогое, как для биржи, так и для ее клиентов».

Что дальше?

В настоящее время основной ЦОД Московской биржи размещен на площадке DataSpace. Там находится ядро торговых систем, а также зал colocation с оборудованием клиентов. При этом существуют системы, основные серверы которых располагаются на площадке М1 с резервированием в ЦОДе DataSpace.

Собственный ЦОД в Большом Кисловском переулке используется и сегодня, в основном для тестовых систем. «Сначала мы разместили тестовый сегмент в дата-центре DataSpace. Но быстро поняли, что держать тестовые системы в дорогом ЦОДе неправильно. А здесь, на Кисловском, все рядом, и это удобно для тех, кто работает с тестовыми системами», – отмечает С. Кобзев.

Принято считать, что время активной жизни ЦОДа – 10 лет. ЦОД биржи в Большом Кисловском переулке «живет» уже 20 лет. Построен он был очень грамотно, продумана возможность замены отдельных элементов (ИБП, кондиционеров и пр.) без остановки работы. Но нет ничего вечного, концепции меняются, совершенствуются. «Если уж мы двигаемся вперед, оценивая сделанное, учитывая передовой международный опыт, то следует признать, что в современных условиях ЦОД в центре города – не самая правильная вещь. Большая фура не подъедет, сложно подвозить топливо, оборудование. Большой запас топлива не создать – мы с уважением относимся к правилам противопожарной безопасности. Коммуникационные колодцы заполнены почти до отказа, – делится опытом С. Мещерин. – Да и совмещать центральный офис и ЦОД, как показала практика, – не самое лучшее решение».

Сейчас Московская биржа просчитывает различные варианты будущего своей ИТ-инфраструктуры. И сомневаться не приходится, специалисты с огромным опытом, которые успешно развивают систему ЦОДов уже более четверти века, найдут оптимальное решение. ИКС

ЦОД: от царства технологий к бизнес-задаче

Скорость, стоимость и качество в ЦОДостроении – это уже не лебедь, рак и щука из басни Крылова. «Сегодня можно строить быстро, качественно и за разумные деньги», – уверен Роман Шмаков, вице-президент подразделения Secure Power в России и странах СНГ компании Schneider Electric.

– Развитие российской отрасли ЦОДов неразрывно связано с цифровизацией экономики страны. Как вы оцениваете темпы этого процесса?

– Принятием программы «Цифровая экономика РФ» государство задало тренд на цифровизацию в первую очередь госорганов, но его подхватили большинство предприятий и организаций. Ведущие госкорпорации анонсировали цифровые стратегии, в руководстве многих компаний появились директора по цифровизации, что подчеркивает важность этого направления. Первая волна, которую можно назвать волной хайпа, схлынула. Интерес стал более осмысленным, зрелым; выработано более четкое понимание, что такое цифровая трансформация, каковы ее цели и механизмы реализации.

Если сравнивать Россию с западными странами, то по темпам и смелости внедрения цифровых проектов мы не отстаем, но существенное различие кроется в точке старта. Нам приходится проделывать дополнительный путь за счет того, что базы для цифровизации – как технологическая основа, так и человеческий фактор – у нас разные. Например, объем рынка ИТ в США существенно больше, что видно, в частности, по количеству и масштабам дата-центров.

Но и в России появились свои лидеры в сфере цифровизации, причем не по анонсам и намерениям, а по реализованным проектам. Это, конечно, Сбербанк, который объективно входит в число мировых лидеров финтеха. Более того, он популяризирует цифровые сервисы среди населения и малого бизнеса. Из госструктур выделяется ФНС, последовательно и успешно внедряющая цифровые сервисы, которые уже дали огромный экономический эффект, в том числе в части возврата НДС. В индустриальном сегменте один из лидеров – «Сибур». Цифровизация ряда ключевых процессов, создание цифровых двойников и другие проекты цифровой трансформации способствовали серьезному повышению операционной устойчивости, конкурентоспособности, снижению издержек.

– Целая группа новых игроков выходит на рынок услуг ЦОДов и облачных сервисов. Среди них и телеком-компании, и финансовые организации. Возможно, на этот рынок выйдут и госкорпорации, многие из которых сейчас находятся на стадии разработки концепции своего цифрового развития. Как это меняет отрасль ЦОДостроения?

– Для большинства новых игроков ЦОДы – это не colocation, а облачные услуги и цифровые сервисы. Если раньше, лет десять назад, компании строили ЦОДы ради консолидации ИТ-ресурсов, то сейчас это промежуточное звено для достижения других целей – цифровизации, предоставления новых услуг и пр.

Новые игроки не готовы тратить годы на создание дата-центров. Они формируют спрос на решения, которые можно быстро проектировать и разворачивать, легко масштабировать. Для нас это очень позитивный тренд, поскольку Schneider Electric всегда уделяла много внимания гибким, легко масштабируемым эффективным решениям. И все наши новые продукты учитывают этот тренд.

Другой интересный момент связан с тем, что многие игроки, намеренные предоставлять цифровые сервисы, рассматривают варианты не только создания своих ЦОДов, но и использования коммерческих площадок. В стране уже построены крупные коммерческие дата-центры, с большинством из которых мы успешно сотрудничаем, причем как в части поставок инженерного оборудования, так и в части предоставления сервисов проектирования и обслуживания.

Новые игроки часто не являются профессионалами в сфере проектирования, строительства и эксплуатации ЦОДов, поэтому растет спрос на экспертов в этих областях. Более того, интеграторы и крупные производители, которые работают в данной сфере, должны уметь не только создавать инфраструктуру, но и осуществлять инжиниринг бизнес-процессов. Становится востребованной более глубокая компетенция, чем просто системная интеграция. Компаний с такой компетенцией пока немного.

– В предыдущем году активизировались региональные проекты ЦОДов. Спецификой таких проектов является дефицит квалифицированных кадров на месте. Отсюда – интерес к комплексным проектам под ключ. Предлагаете ли вы подобные решения?

– Да, мы тоже видим повышенный интерес к законченным решениям под ключ – будь то полноценный модульный ЦОД или микроЦОД. И нам есть что предложить заказчикам. Главное – мы не пытаемся навязать готовое решение, мы всегда учитываем все требования и замечания заказчика и, основываясь на нашей многолетней экспертизе, создаем законченное решение, которое будет наиболее эф-

Реклама

фективно решать его задачу. Это позволяет снизить расходы как на этапе закупки оборудования, подготовки площадки, коммуникаций, так и при эксплуатации. О том, что мы чрезвычайно внимательно относимся к надежности предлагаемых решений, я даже говорить не буду – все наши заказчики знают об этом, и потому работают с нами уже много лет, а некоторые – десятилетий.

В условиях цифровой трансформации все большему числу заказчиков требуются не монообъекты, а гибридные архитектуры с крупными ЦОДами в центре и большим числом распределенных edge-объектов. В подобных архитектурах предъявляются новые требования к отказоустойчивости и стандартизации (типизации) решений. Такие сети ЦОДов востребованы транспортными компаниями, в горнодобывающей, нефтегазовой отраслях, здравоохранении – везде, где имеется географически распределенная структура.

– Быстрота реализации проекта – это замечательно, но при этом требования к качеству и надежности по меньшей мере не снижаются?

– Только повышаются. Когда людям, отвечающим за цифровизацию госорганов, и владельцам коммерческих компаний я задаю стандартный вопрос о приоритетах, они в первую очередь говорят о высокой доступности сервисов и отказоустойчивости ЦОДов. Важность обслуживаемых ИТ-системами процессов растет экспоненциально, все больше заказчиков выражают нулевую толерантность к сбоям в работе ЦОДа.

В связи с возросшей критичностью распределенных узлов сегодня к ним предъявляются те же требования по резервированию инженерных систем, что и в мегаЦОДах. Но если говорить о сети ЦОДов, то критерии оценки ее отказоустойчивости, конечно, отличаются от критериев, применяемых к монообъектам. Например, в некоторых проектах удобнее резервировать не инженерные системы одного edge-ЦОДа, а edge-узел целиком. Существуют и другие методы повышения надежности системы из множества объектов.

– Получается, сегодня заказчикам нужны высокие скорость и качество реализации ЦОДа, но по приемлемой стоимости. Разве можно в одном проекте реализовать все три требования – они кажутся взаимоисключающими?

– Скорость, стоимость и качество в области ЦОДостроения – это уже не лебедь, рак и щука из басни Крылова. Можно ли быстро, качественно и за разумные деньги построить ЦОД? Без сомнения, можно. Но для этого нужен соответствующий подход у заказчика. Ведь нередко в организации бюджеты на строительство и эксплуатацию находятся в разных руках. Чтобы достичь поставленной цели, необходимо еще на уровне концепции ЦОДа держать в уме его будущую эксплуатацию. Нужно понимать, что капитальные и эксплуатационные затраты неотделимы друг от друга. Важно рассматривать общую стоимость владения (TCO), и все больше заказчиков это понимают.

Поясню на примере. Сейчас трендом рынка ИБП является внедрение литий-ионных батарей. Безусловно, капитальные затраты на них существенно выше, чем на обычные свинцово-кислотные АКБ. Но если посчитать полную стоимость 10-летнего жизненного цикла связки ИБП и батарейного массива, включая затраты на замену батарей, обслуживание и аренду помещений для ИБП и последующую утилизацию АКБ, то оказывается, что для литий-ионных батарей она ниже.

Недавно мы реализовали проект поставки ИБП на литий-ионных батареях в ЦОД одного из ведущих банков страны. Такие батареи были выбраны не случайно – оборудование нужно было поднимать и устанавливать на 24-м этаже, благодаря своему малому весу они отлично для данной задачи подошли. Для финансовой организации риски, связанные с нарушением работы ИТ-сервисов, огромны, поэтому требования к надежности были самыми высокими. Сроки реализации проекта были сжатыми. Но все три условия – скорость, стоимость и качество – были успешно выполнены. И, поверьте мне, этот заказчик как никто другой умеет считать деньги. Кстати, для оптимизации затрат и сроков поставки в проекте использовались ИТ-стойки Schneider Electric локального производства.

– Помимо трех ключевых параметров, которые мы обсудили, важна еще и эффективность ЦОДов. Что с этим показателем?

– Задачи повышения эффективности стоят в любой организации. Говоря о ЦОДах, можно отметить, что на уровне отдельно взятой инфраструктуры или системы возможности повышения эффективности во многом исчерпаны. Например, КПД ИБП уже близок к 100%. Дополнительные возможности связаны с синергией взаимодействия разных систем.

У нас есть технологическая платформа EcoStruxure. С ее помощью можно объединить все элементы производственной и энергетической инфраструктуры на цифровом уровне и эффективно управлять активами – от подключенных устройств до цифровых аналитических приложений.

Сегодня отношение к ЦОДам меняется. Раньше они были своеобразными «космическими кораблями», квинтэссенцией технической мысли, гордостью инженеров и царством технологий. Сейчас ЦОД для все большего числа заказчиков становится объектом бизнеса, инструментом с определенными бизнес-параметрами. В этой парадигме способность ЦОДа и его элементов «находиться в диалоге» с инфраструктурой предприятия очень важна. И концепция EcoStruxure – как раз не про соединение разного оборудования, а именно про диалог разных систем: ИТ, инженерных сетей, производственных и бизнес-процессов.

Цифровой диалог ЦОДа с другими системами не только существенно повышает эффективность самих дата-центров, но и является необходимым элементом сквозной цифровизации и повышения эффективности предприятий.

Life Is On Schneider Electric
www.schneider-electric.ru

Реклама

Edge-ЦОДы в многофункциональных зданиях

Ричард Ван Лу, вице-президент, Uptime Institute
Кевин Хеслин, главный редактор, Uptime Institute Journal

Размещение дата-центров в многофункциональных зданиях может дать операторам и владельцам ЦОДов определенные выгоды, нужно только не забывать о сопряженных с таким подходом рисках.

Концепция граничных вычислений предполагает использование небольших ИТ-комплексов, которые служат для распределения нагрузки или приближения ИТ-сервисов к конечным потребителям. При этом ИТ-оборудование может размещаться в зданиях смешанного назначения, например, в удаленном офисе или многофункциональном здании, а не в специализированном центре обработки данных. В некоторых случаях эти комплексы могут состоять всего из нескольких стоек, но их безопасность, доступность и управляемость очень важны.

При размещении в многофункциональных зданиях небольшие ИТ-объекты часто используют не предназначенные для критических потребителей помещения и ресурсы совместно с другими системами здания. В этих случаях, чтобы организовать доступ к ИТ-оборудованию для технического обслуживания и к таким общим ресурсам, как комнаты для переговоров или зоны разгрузки, может понадобиться специальное планирование. Подобное размещение ИТ-комплексов предъявляет особые требования к обеспечению безопасности. А владельцам и операторам небольших ЦОДов может оказаться сложнее или дороже реализовать соответствие определенному уровню (Tier) Uptime Institute.

По мере развития ИТ-комплексов в направлении распределенных архитектур критически важные активы все чаще размещаются в филиалах или удаленных офисах. В одних случаях ИТ-объекты переносят в удаленные, более безопасные места для защиты от вандализма, неблагоприятных погодных условий или происшествий. В других – ИТ-шкафы устанавливают ближе к пользователям, в офисах обслуживания или учреждениях, работающих с клиентами. Часто они оказываются вне контроля центрального ИТ-отдела и обслуживаются местными специалистами. Но сегодня ИТ имеют решающее значение для функционирования бизнеса, и необходимо, чтобы ИТ-отделы четко контролировали состояние и работу своих систем.

В многофункциональных зданиях по экономическим или иным причинам иногда размещают и относительно крупные ИТ-комплексы. Такие компании, как Facebook, придерживаются подобного подхода для управления расхода-

ми на недвижимость, полагая, что использовать 1000 кв. м для ИТ-систем в частично занятом здании дешевле, чем арендовать ЦОД или строить его с нуля. В других случаях руководству ИТ-подразделения просто неудобно, чтобы серверы находились слишком далеко от конечных пользователей или корпоративного надзора.

Так или иначе небольшие ИТ-объекты, как правило, являются частью среды смешанного использования наряду с помещениями и ресурсами, предназначенными для производства, транспортировки, обслуживания клиентов и т.п., например в отделениях банков. В этих условиях возникают задачи защиты критически важных ИТ-активов от процессов, происходящих в коммерческих зданиях, поддержания целостности операций, бюджетов, доступа, безопасности и даже процедур обслуживания. ИТ-активы, расположенные в средах общего пользования, часто должны использовать ресурсы объекта совместно с другими системами, что создает дополнительный ИТ-риск. Риск повышен во всех смешанных средах, но особенно в коммерческих, производственных и промышленных условиях.

Общие рекомендации

При размещении ИТ-комплексов на многофункциональных объектах Uptime Institute рекомендует следующее:

- Не допускать, чтобы какие-либо некритические мероприятия имели приоритет более высокий, чем критически важные ИТ-процедуры.
- Разделять бюджеты, выделяемые на ИТ-нужды и на все остальное.
- Разъяснять всем находящимся в здании субъектам важную роль ЦОДа в деятельности компании (организации).
- Разработать обязательные для исполнения правила, ограничивающие доступ к ИТ-активам.
- Распланировать доступ к общим объектам, включая зоны разгрузки, складские помещения и переговорные комнаты.
- Учитывать законные потребности в комфортных условиях работы других пользователей в общем пространстве.
- Заранее определить периоды технического обслуживания с учетом выходных и праздничных дней.

Потеря доступа к своим данным, даже на короткое время, серьезно сказывается на многих компаниях. Некоторые настолько полагаются на данные, что из-за потери доступа к ним их дальнейшее существование может быть поставлено под угрозу. Понимание руководством этих вроде бы очевидных вещей поможет выполнить требования системы Tier.

Риски и возможности

Более 60% организаций, опрошенных Uptime Institute в 2019 г., эксплуатируют малые или микрообъекты ИТ, которые могут размещаться в многофункциональных зданиях (рис. 1). Растущее использование граничных вычислений предполагает, что в будущем эта доля может увеличиться. А значит, все более важно, чтобы критические ИТ-комплексы, расположенные в общих пространствах, были сконфигурированы, управлялись и обслуживались в соответствии с бизнес-требованиями.

Размещение ИТ-комплекса на многофункциональном объекте имеет свои плюсы и минусы. ЦОДы, особенно построенные для предоставления услуг colocation, часто имеют вспомогательные помещения, предназначенные для использования ИТ-службами, например, переговорные, зоны разгрузки, склады, а также соответствующие обслуживающий персонал и бюджет. Но эти ресурсы нередко недостаточны или ограниченны.

Рис. 1. В каких средах располагаются ИТ-ресурсы организаций ▼

62% МикроЦОДы (т.е. комплексы «все в одном», включающие системы питания, охлаждения и стойки с мощностью, как правило, до 150 кВт) в собственности компании

66% Серверные комнаты или распределенные ИТ-комплексы в собственности компании или являющиеся частью корпоративных активов

Показаны не все варианты ответов

Источник: Uptime Institute Global Survey of IT and Data Center Managers, 2019, n = 696

В некоторых ЦОДах нет переговорных комнат, поэтому встречи проводятся там, где можно обеспечить необходимую конфиденциальность, иногда без досок, проекционных дисплеев и другой электроники для заметок или поддержки конференц-звонков. В других ЦОДах отсутствуют достаточные складские или разгрузочные площадки, что затрудняет инвентаризацию запасных частей или выполнение масштабных проектов модернизации.

В то время как многофункциональные среды обычно включают все эти удобства, они не закреплены полностью или хотя бы частично за критически важными ИТ-задачами. Это может означать, что ИТ-менеджерам потребуется планировать встречи заранее, находить способы обеспечения безопасности оборудования, хранящегося в общих пространствах, и координиро-

вать свои действия с другими отделами, например, в отношении использования зон разгрузки. Совместно могут потребляться и другие ресурсы: подключения к сетям связи, водоснабжение, электропитание, вентиляция и охлаждение.

Недостатки, обусловленные совместным использованием объекта, могут быть несколько компенсированы усилением влияния ИТ в корпоративной среде. Скажем, общая парковка или кафетерий могут сблизить отделы и сотрудников, так что каждый будет лучше понимать и ценить работу других. ИТ-специалисты смогут узнать от коллег из других отделов об их ИТ-потребностях или об общей организации компании. А офисные сотрудники смогут понять, почему ИТ-службы получают столь большую часть бюджета, почему ИТ-специалисты часто трудятся в нерабочее время и почему им постоянно требуются новые и все более сложные ИТ-инструменты. Еще большее взаимопонимание могут обеспечить экскурсии в ЦОД, во время которых руководители и другие сотрудники узнают о том, как функционируют ИТ-системы, например, при обслуживании клиентов или выполнении офисных задач.

Однако повышенная открытость ИТ-объекта имеет и оборотную сторону. Множество посторонних людей – вероятно, самая большая проблема для многофункциональных зданий. В таких условиях ИТ-отдел должен досконально проработать правила доступа, четко контролируя время, объем, условия и продолжительность визитов внешних посетителей. Проблемой могут стать, например, генеральный директор, который хочет быть выше всех правил, или уборщики, которые легко меняются сменами или обслуживаемыми помещениями.

Люди почти всегда оказываются самым серьезным риском, с которым сталкиваются ЦОДы, но на многофункциональных объектах риск возрастает по причине близости к дата-центру большого числа неквалифицированных людей. Возможно, ИТ-отделу удастся исключить саму возможность проникновения этих людей в помещения ЦОДа, но он не сможет контролировать события, происходящие в соседних помещениях, – например, празднование дня рождения, которое может привести к тому, что развеселившиеся сотрудники случайно активируют пожарную сигнализацию с последующей эвакуацией всего здания.

С учетом потребностей других

Потребности пользователей здания могут оказать влияние на график работ, связанных с ИТ-системами. Техническое обслуживание и модернизация ЦОДа должны координироваться с другими работами, проводимыми в здании. Некоторые мероприятия по техническому обслуживанию ИТ-комплексов могут привести к временному прекращению функционирования системы комфортного кондиционирования, повышению нагрузки на электросеть или проблемам с доступом в интернет, поэтому их придется отложить или запланировать на нерабочее время.

Шум – это еще одна проблема. При некоторых планировках здания даже крупные поставки оборудования для ЦОДа, возможно, придется отложить, чтобы избежать негативного воздействия шума из зоны разгрузки.

ИТ-комплекс также должен существовать в рамках ограничений, налагаемых особенностями здания, включая его системы безопасности жизнедеятельности и управления. Обе эти системы разработаны в первую очередь для удовлетворения потребностей людей, находящихся в здании. Только после того, как эти приоритеты будут соблюдены, можно говорить о регулировании температуры, изменении процедур обеспечения безопасности и маршрутов аварийного выхода в соответствии с требованиями ИТ.

Эксперты Uptime Institute рекомендуют, чтобы системы, имеющие отношение к ИТ, были максимально независимы от общих систем здания. Это одна из причин, по которой мы уже давно выступаем за отдельные ЦОДы. Но мы понимаем, что полного разделения никогда не было и, вероятно, никогда не будет.

Переезд в существующее здание

Переезд ИТ-систем в существующее многофункциональное здание означает, что его инфраструктура должна быть серьезно модернизирована. Поскольку «новые» пространства обычно не являются новыми, требования ИТ могут оказаться невыполнимыми, и понадобится искать компромисс. Например, иногда невозможно создать отдельный вход для ИТ-объекта или даже обеспечить должную безопасность главного входа.

Кроме того, здание, в котором будет размещен новый ИТ-комплекс, должно пройти обширную и, возможно, очень дорогую модернизацию системы распределения электроэнергии для обеспечения двух лучей подачи электропитания (A&B) для серверов с двумя шнурами питания. На тесных площадках возникает соблазн установить один дизель-генератор для питания как ИТ-, так и некритических нагрузок. Но такое решение может привести к дисбалансу при обслуживании нагрузок. Одна из имеющихся альтернатив – установка второго, меньшего генератора, но здесь надо учитывать, что наличие генераторов разного размера может вызвать проблемы синхронизации. Если необходимо выполнить требования Tier III или Tier lV, понадобится более серьезная модернизация.

Наконец, простое увеличение производительности систем непосредственного охлаждения, распространенных в коммерческих зданиях, способно ограничить плотность мощности ИТ-оборудования даже после обширной реконструкции. Во всех этих случаях добавление необходимых систем и подсистем не обязательно избавит от общей инфраструктуры, которая может сделать недостижимым получение сертификата Tier III или Tier IV.

В дополнение к ограничениям мощности и емкости планировка здания таит множество других рисков. Например, легковоспламеняющиеся офисные принадлежности могут храниться рядом с критически важными ИТ-помещениями, а над ИТ-оборудованием могут размещаться водопровод для офисных кухонь, системы пожаротушения или туалеты. Такие ситуации не исключены даже в хорошо спроектированных зданиях.

Не затеряться в общем здании

Руководители могут видеть в ИТ-комплексе просто еще одну функцию здания, в котором ЦОДу придется постоянно бороться за поддержание целостности своих систем. Это особенно часто случается, когда бюджеты ИТ- и других служб здания объединены. Uptime Institute рекомендует, чтобы ЦОД имел отдельный годовой и пятилетний бюджеты на капитальные и операционные расходы, чего, правда, непросто добиться на объекте смешанного использования.

Однако в равной степени верно и то, что руководство может рассматривать резервное электропитание, охлаждение и выделенный персонал как ресурсы, которые должны использоваться совместно на благо всех, особенно если системы не являются достаточно независимыми и не снабжены средствами детализированного мониторинга. Идея загрузить системы бесперебойного питания более чем на 45–50% может быть привлекательной для менеджеров, стремящихся повысить общую эффективность объекта.

Аналогичная ситуация может возникнуть и с общим персоналом. Когда рутинные задачи технического обслуживания здания возлагаются на высококвалифицированных сотрудников, нацеленных на работы с критически важными ИТ-системами, профилактическое обслуживание последних и другие процедуры порой нарушаются или переносятся на более поздний срок. Возложение на персонал обязанностей, не связанных с ИТ, может привести не только к более частым сбоям из-за отложенного обслуживания, но и к более длительным простоям, поскольку сотрудники будут не готовы к немедленному реагированию.

Даже подготовленный для ИТ-оборудования фальшпол может оказаться под угрозой, особенно когда требования к площади других бизнес-единиц растут быстрее, чем ИТ-отдел занимает отведенные ему площади.

▲ **Экскурсия в ЦОД позволит его соседям по многофункциональному зданию лучше понять важность ИТ**

Все не так грустно

Удовлетворение растущих требований к производительности ИТ-комплексов для граничных вычислений не будет безболезненным. Более высокие требования к ИТ делают отказоустойчивость и доступность еще более критичными, и новые архитектуры, вероятно, будет непросто реализовать.

Организациям уже сейчас нелегко размещать ИТ-комплексы на многофункциональных объектах без ущерба для критически важных ИТ-сервисов. Для устранения возникающих проблем необходимо создавать адекватную инфраструктуру на каждом объекте, разрабатывать и выполнять соответствующие бюджеты и процедуры, а также содержать ИТ-активы в контексте других приоритетов организации.

Однако совместное использование пространства и ресурсов на многофункциональном объекте может повысить престиж ИТ-служб и улучшить понимание того, как ИТ помогают достигать бизнес-целей. Это будет способствовать усилению поддержки со стороны руководства и даже упростит финансирование важных проектов.

В ближайшей перспективе операторы датацентров должны подготовиться к тому, что ИТ-комплексы будут все чаще размещаться на многофункциональных объектах. Признание потребностей других пользователей и систем здания – хороший первый шаг к минимизации их воздействия на функционирование ИТ-комплекса. Кроме того, ИТ-отделы должны постараться понять, как извлечь выгоду из сосуществования в среде смешанного назначения и сохранить высокий приоритет ИТ. ИКС

Суперкомпьютеры: схватка тяжеловесов

Николай Носов

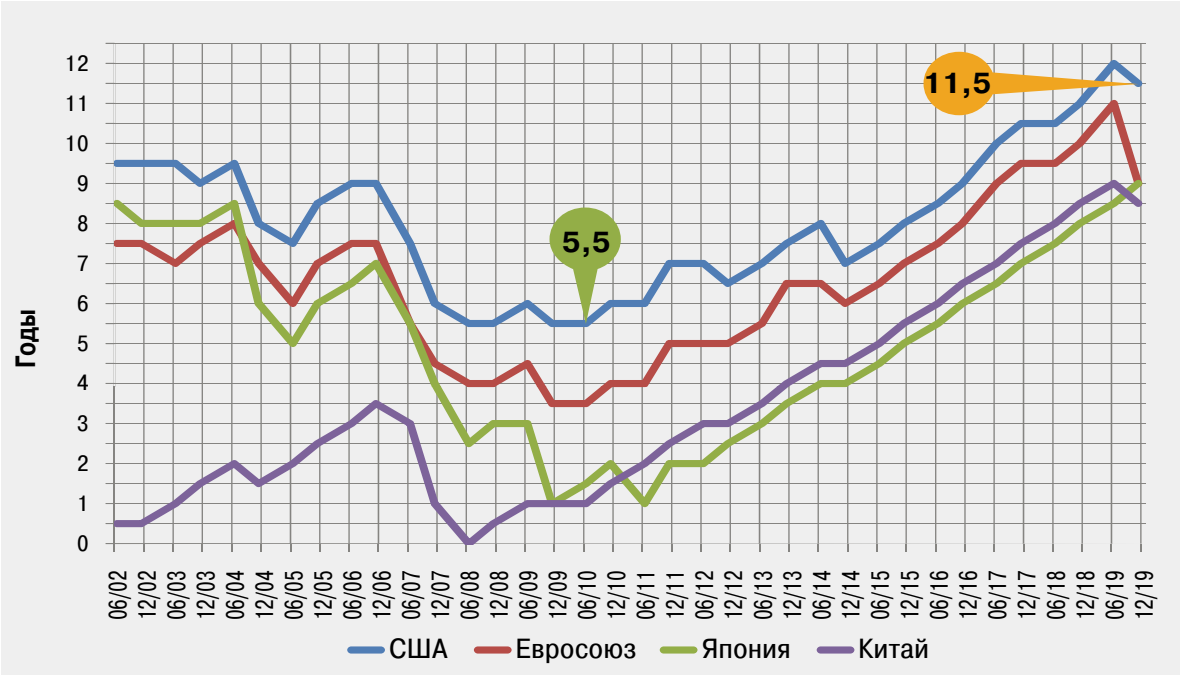
В список Top500 самых мощных публичных вычислительных систем мира включен третий российский суперкомпьютер, но отставание нашей страны от лидеров по-прежнему велико.

Новости российского рынка

Попадание суперкомпьютера Christofari, представленного Сбербанком, в ноябрьский список Top500 самых мощных вычислительных систем мира стало хорошей новостью к открытию Национального суперкомпьютерного форума. Самый мощный российский суперкомпьютер занял почетное 29-е место. Это третья российская система в престижном мировом рейтинге суперкомпьютеров.

Названный в честь первого клиента сберегательных касс России Николая Кристофари, памятник которому стоит перед главным офисом Сбербанка в Москве, суперкомпьютер предназначен в первую очередь для задач искусственного интеллекта. Вычислительная система создана на базе высокопроизводительных узлов Nvidia DGX-2. В ней используются процессоры Intel Xeon Platinum 8168 24C 2,7 Гц и межузловая шина (интерконнект) Mellanox InfiniBand EDR. Производительность Christofari по тесту LinPack составляет 6,669 петафлопса.

Приятная новость не меняет общую картину. Отставание от лидеров – США и Китая – по-прежнему велико. Так, возглавляющий гонку американский суперкомпьютер Summit имеет производительность 148 петафлопс, идущий на третьем месте китайский Sunway TaihuLight – 93 петафлопса. Да и сам компьютер Сбербанка – импортного производства. Наша доля в совокупной мировой производительности суперкомпьютеров



Отставание России по ∑Rmax от США, Евросоюза, Китая и Японии ▶

(ΣRmax) всего 0,63%. Причем, если отставание России от США по суммарной производительности суперкомпьютеров в 2010 г., по оценкам Сергея Абрамова, директора Института программных систем им. А.К. Айламазяна РАН, составляло пять лет, то в нынешнем – уже 11 (см. рисунок).

В результате индекс цифровизации, вычисляемый как отношение доли страны в суммарной производительности суперкомпьютеров мира к доле страны в мировом ВВП, у России в 6 раз ниже, чем у Китая, в 4 раза – чем у США, в 3 раза – чем у Японии и вдвое ниже, чем у Евросоюза (см. таблицу).

Эксперт отметил и несбалансированность российского рынка. Если у ведущих стран использование вычислительных мощностей в основном приходится на науку и разработку, причем именно государство финансирует работы по созданию суперкомпьютеров и предоставляет к ним доступ, то самый мощный российский компьютер принадлежит банку и будет использоваться для решения его задач. Сторонние организации в лучшем случае смогут получить доступ к Christofari на коммерческой основе.

Эксафлопсная эра

Производительность самой мощной вычислительной системы мира до 2008 г. увеличивалась в тысячу раз каждые 11 лет. Однако на рубеже 2008 г. мировая суперкомпьютерная отрасль столкнулась с научно-техническими сложностями, темп замедлился, и теперь ожидается, что тысячекратное увеличение произойдет на отрезке более 17 лет.

В результате прогнозы достижения новых рубежей производительности пересматриваются. Если не произойдет какого-либо технологического прорыва, то 1 эксафлопс, скорее всего, будет покорен в 2022 г., а 1 зеттафлопс – после 2039 г.

В гонке супертяжеловесов лидерство после нескольких лет побед Китая вернулось к США, которые собираются первыми войти в эксафлопсную эру. В марте минувшего года Министерство энергетики США объявило, что Intel и Cray построят первый в стране эксафлопсный суперкомпьютер Aurora, который будет установлен в Аргоннской национальной лаборатории в 2021 г. В мае министерство сообщило, что AMD и Cray создадут суперкомпьютер Frontier для Оук-Риджской национальной лаборатории. Ожидается, что суперкомпьютер с вычислительной мощностью 1,5 эксафлопса начнет работать в 2021 г. В августе Министерство энергетики США, Национальная администрация по ядерной безопасности и Ливерморская национальная лаборатория им. Лоуренса подписали контракты с Cray на создание первого суперкомпьютера Национальной администрации по ядерной безопасности – El Capitan. Запуск запланирован на конец 2022 г., максимальная производительность превысит 1,5 эксафлопса.

Страна	Доля ΣRmax, %	Доля ΣВВП, %	Индекс
Китай	32,29%	14,84%	2,18
США	37,10%	24,32%	1,53
Япония	6,65%	5,91%	1,13
Евросоюз	17,74%	21,37%	0,83
Россия	0,63%	1,80%	0,35

Источник: материалы НСКФ, 2019

Индекс цифровизации, ноябрь 2019

В сентябре 2019 г. компания HPE купила Cray и теперь сама займется реализацией амбициозных проектов. По словам представителя HPE, в трех новых строящихся в США эксафлопсных суперкомпьютерах будут использоваться последние технологии процессоров и графических ускорителей компаний AMD и Intel и интерконнект Slingshot от Cray, ныне принадлежащей HPE. Прогнозируется, что каждая из машин поочередно возглавит список Top500, а суммарная мощность трех суперкомпьютеров втрое превзойдет суммарную производительность всего текущего Top500.

> Надо провести адекватную оценку дел, разработать сбалансированную государственную программу и заново создать национальную суперкомпьютерную инфраструктуру, доступную всем научным и коммерческим организациям как «общественное благо». Решающая роль в ее создании должна принадлежать государству.

Сергей Абрамов, директор Института программных систем им. А.К. Айламазяна РАН

Речь идет о новых GPU известных брендов. Среди актуальных решений для гибридных систем на сегодня лидируют ускорители Nvidia — 35% ΣRmax, в то время как текущие успехи графических ускорителей AMD и Intel на рынке суперкомпьютеров скромные — на долю Intel приходится менее 1% ΣRmax, а компания AMD совсем исчезла из списка. Отдельно стоит упомянуть новые ускорители PEZY Computing (Япония), Matrix-2000 (Китай) и Deep Computing Processor (Китай) с заметной совокупной долей 7% ΣRmax.

Сделаем сами

Критическую важность для суперкомпьютеров имеют технологии интерконнекта, причем лидеры рейтинга Top500 используют собственные решения, недоступные на рынке. России придется разрабатывать их самой. Но, как заявил С. Абрамов, такая разработка нашим специалистам по силам и не раз уже успешно выполнялась. ИКС

СХД для систем видеонаблюдения

Сергей Орлов, независимый эксперт

Системы видеонаблюдения сегодня востребованы во многих отраслях. С увеличением масштабов развертывания таких систем и плотности размещения камер растут и объемы генерируемых ими данных.

Емкость и стоимость

Разрешение камер продолжает расти, и это позволяет увеличить изображение для более качественного и надежного распознавания лиц или номерных знаков, повышает точность систем видеоаналитики. Но вместе с разрешением растут и требования к емкости и производительности систем хранения, полосе пропускания сети.

Согласно оценкам компании Seagate Technology, в 2023 г. объем данных, которые в течение одного дня будут генерироваться во всем мире установленными за последний год камерами видеонаблюдения, достигнет 3500 Пбайт.

Проблема усугубляется тем, что ввиду террористических атак многие страны обязывают хранить записи систем видеонаблюдения в течение все более длительного периода времени. В зависимости от отрасли и нормативных требований срок хранения видеоархива может варьироваться от месяцев до лет. Например, правила многих аэропортов требуют, чтобы зафиксированные на видео события хранились в течение семи лет и более. А типичный аэропорт продуцирует сотни гигабайт видео в день.

Таким образом, хранение данных играет в системах видеонаблюдения жизненно важную роль. Инфраструктура хранения должна также обеспечивать поиск видео, чтобы пользователи могли быстро получать определенные фрагменты для просмотра. Нередко такие данные используются в системах видеоаналитики и должны быть доступны для анализа с помощью алгоритмов машинного обучения/ИИ.

В результате заметная доля бюджета всего проекта видеонаблюдения приходится именно на системы хранения. По некоторым оценкам, стоимость СХД может достигать 20% и более общей стоимости системы.

Согласно недавнему отчету MarketsandMarkets, мировой рынок видеонаблюдения вырастет с почти $37 млрд в 2018 г. до более чем $68 млрд в 2023 г. В основном этот рост обусловлен продолжающимся переходом от аналоговых систем видеонаблюдения к системам на основе IP. Снижение стоимости IP-камер способствует широкому применению этих систем во всем мире, подстегивая спрос на качественные и экономичные решения для хранения данных, благодаря чему рынок растет со скоростью 25% в год (рис. 1).

Однако с учетом быстрого роста объема видеоданных задача создания систем видеонаблюдения, позволяющих оптимально удовлетворить потребности заказчика и одновременно сбалансировать затраты и удобство использования, становится все сложнее. Одно из самых больших препятствий – стоимость хранения видеоданных.

Требования к СХД

Требования к системе хранения данных определяются спецификой систем видеонаблюдения, а именно:

- однородностью данных;
- относительно постоянной и интенсивной нагрузкой;

● превалированием режима записи. Чтение видео для просмотра или анализа осуществляется значительно реже;
● необходимостью функционирования в реальном времени.

В общем случае СХД для системы видеонаблюдения должна обладать такими качествами, как эффективность работы с последовательными нагрузками, экономичность масштабирования при увеличении количества видеокамер и/или емкости архива, способность справляться с ростом нагрузки, незначительная (в пределах 10%) потеря производительности при отказе накопителей и отсутствие потерь данных при отказах. Принципиальное значение имеют запас пропускной способности СХД, стабильность доступа к данным и возможность достоверного восстановления событий.

В крупных проектах необходимы высокая скорость работы с видеопотоками, поддержка большого числа камер с разрешением до Full HD/4K, гибкое масштабирование решения с ростом требований, параллельное чтение данных без потери производительности на запись (для работы приложений видеоаналитики), эффективное функционирование в многопоточном режиме и при пиковых нагрузках.

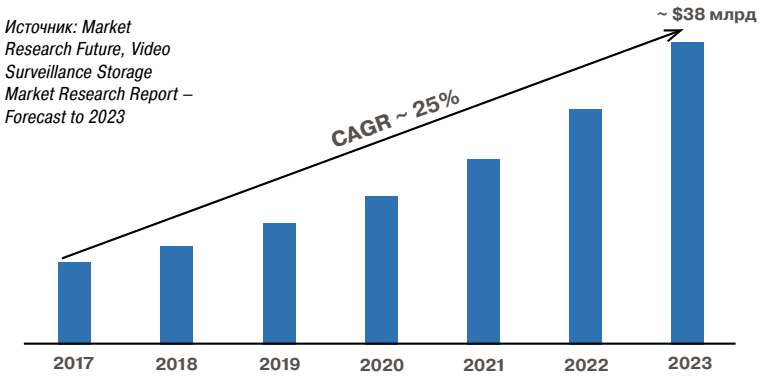
Повышенный уровень доступности и целостности данных СХД достигается за счет быстрой реконструкции RAID-массива, использования уровней RAID повышенной надежности, например RAID 7.3 или RAID N + M (RAID 7.3 – аналог RAID 6, но с более высокой надежностью благодаря расчету сразу трех контрольных сумм). Единая точка отказа системы хранения устраняется в двухконтроллерной конфигурации active-active.

Для систем видеонаблюдения характерны многопоточные последовательные операции ввода/вывода, поскольку каждая IP-камера создает последовательный поток данных для записи в хранилище. В результате формируется многопоточная нагрузка на запись (более 90% операций) и незначительная нагрузка чтения – один или более потоков для просмотра видео из архива.

Поэтому для задач видеонаблюдения обычно выбирают не самые производительные и относительно недорогие массивы большой емкости на HDD. Такие бюджетные решения могут представлять собой СХД вендоров второго эшелона либо массивы на стандартном серверном оборудовании и программно определяемые СХД (Software Defined Storage, SDS).

NAS и DAS

Одним из решений является хранение данных в сетевых хранилищах (Network Attached Storage, NAS). Это означает централизованное администрирование и хранение данных с совместным доступом или выделением томов (Logical Unit, LUN) для каждого сервера видеонаблюдения и подключение сервера к LUN через локальную сеть (например, по протоколу iSCSI).



▲ **Рис. 1. Прогноз роста мирового рынка СХД для систем видеонаблюдения**

Создание системы видеонаблюдения на основе серверов NAS во многих случаях – оптимальный вариант, особенно в масштабных проектах. Сервер NAS выступает центральным элементом инфраструктуры видеонаблюдения, обеспечивающим хранение и обработку видеоданных с камер. Использование серверов NAS снимает проблему централизованного хранения и просмотра видео, так как они приспособлены для работы в распределенных сетях.

К основным преимуществам NAS для организации видеонаблюдения относят высокую масштабируемость, возможности создания крупных и территориально распределенных систем, интеграции с информационными системами предприятия, совместимость с IP-камерами разных вендоров, высокий уровень безопасности, широкие возможности резервного копирования и аварийного восстановления, выбора и разработки программного обеспечения для NAS, работающих под управлением обычных серверных ОС.

Сервер NAS может не только записывать видеоданные, но и обрабатывать их. С его помощью можно настроить и автоматизировать такие действия, как детекция движения, сценарии с использованием данных с нескольких камер и датчиков, контроль наличия объектов в поле видимости камеры, проверка и корректировка параметров камеры (наклона, фокуса и пр.).

Проблема расширения хранилища видеоданных решается установкой дополнительных дисков (общей емкостью до сотен терабайт) или включением в систему еще одного сервера. Увеличение числа IP-камер и их подключение к серверу займут несколько минут.

Пример подобного решения – совместный продукт компаний Cloudian и Milestone (рис. 2), который предлагается как основа построения систем видеонаблюдения, способных одновременно записывать видео с тысяч камер. В нем плат-

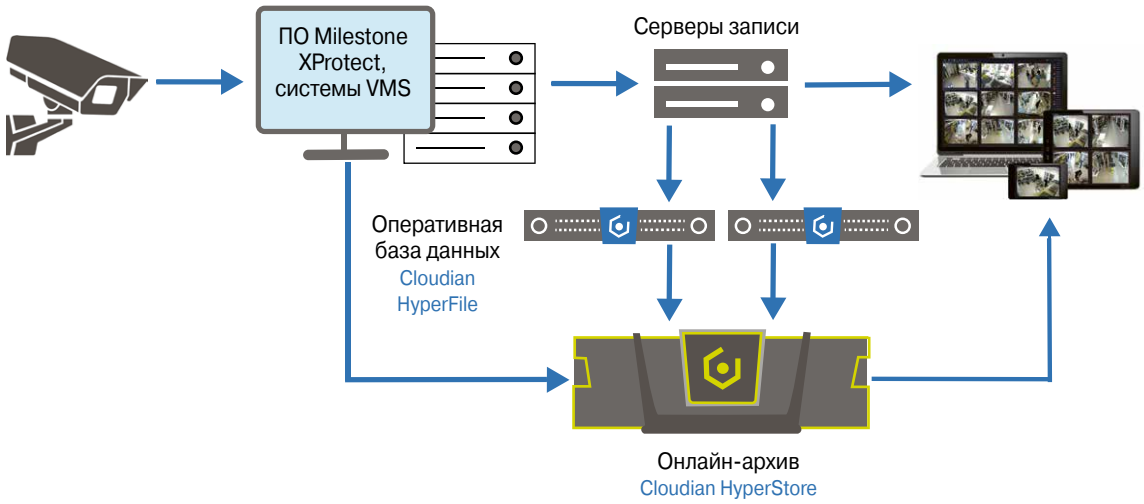


Рис. 2. ▶ Системы хранения Cloudian HyperFile и HyperStore с ПО Milestone XProtect

форма хранения Cloudian интегрирована с ПО Xprotect от Milestone. Такая масштабируемая система может быть распределенной, при этом видео записывается в центральное хранилище. Cloudian HyperFile NFS настраивается как оперативная база данных с архивированием в HyperStore. Видео первоначально сохраняется в оперативной базе данных, а затем перемещается в архивную БД на основе расписания и/или политик, заданных в системе управления видеонаблюдением (Video Management System, VMS). По данным разработчиков, это решение отличается высокой плотностью хранения, оптимизируя затраты на хранение до 70% по сравнению с традиционными сетевыми хранилищами.

Другой вариант распределенной системы предлагает компания Qumulo (рис. 3). Видеозаписи с камер видеонаблюдения разного типа сохраняются в распределенной файловой системе Qumulo и размещаются на разных уровнях хранения: на SSD для оперативной аналитики, на дисках большой емкости или опционально – в облаке.

Dell EMC для хранения данных наблюдения, управления ими и доступа к ним в распределенных системах разработала ряд специализированных продуктов. СХД Unity, поддерживающая работу с терабайтами данных, может использоваться как центральная СХД с блочным доступом. Кластер Isilon NAS с ОС Isilon OneFS позволяет получить масштабируемый пул хранения данных с глобальным пространством имен.

Между тем некоторые специалисты считают применение массивов NAS избыточным и менее надежным, чем систем хранения данных с прямым подключением (Direct Attached Storage, DAS). DAS подразумевает прямой доступ сервера к СХД или размещение дисков внутри сервера и их объединение в RAID-массив с целью увеличения производительности и отказоустойчивости системы хранения. Прямое подключение к дисковому массиву считается самым надежным, поскольку обеспечивает постоянный гарантированный доступ ко всем записанным данным, сохранению которых не помешают потенциальные проблемы в сети. Да и стоимость хранения может получиться более низкой. Кроме того, исключается единая точка отказа.

Рис. 3. Поток данных в системе видеонаблюдения Qumulo ▼

Для масштабирования такой системы увеличивают число серверов с локальными СХД и/или наращивают емкость СХД-сервера добавлением полок с дисками JBOD.

Другой вариант – комплексные «коробочные» решения. Примером может служить видеосервер Divitec (рис. 4), готовая система видеонаблюдения с ПО Divitec под ОС Linux. Он позволяет одновременно просматривать видео в реальном времени, записывать архив, просматривать видео из архива, осуществлять резервное копирование и удаленный доступ. Видеосервер поддерживает IP-камеры разных вендоров по протоколу Onvif 2.3, использует формат сжатия видео H.264. Максимальный поток – до 300 Мбит/с.

SDS в системах видеонаблюдения

Программно определяемые СХД (SDS) эффективно работают на стандартном серверном оборудовании, достаточно легко встраиваются в существующую ИТ-инфраструктуру и снижают издержки за счет простого масштабирования. Как правило, они предоставляют широкие возможности конфигурирования и настройки под конкретные задачи, позволяют реализовывать масштабные и нестандартные проекты. Они могут предусматривать интерфейсы для подключения к сети SAN и/или NAS (Ethernet, InfiniBand, FC), прямое подключение к хостам (DAS) по протоколам SAS или iSCSI.

Такой вариант особенно подходит для небольших и некритичных проектов в условиях ограниченного бюджета. Для систем, где нужны гарантированная надежность, производительность, отказоустойчивость и сервис, предпочтительнее традиционные решения ведущих вендоров.

Программные СХД позволяют создавать производительные и отказоустойчивые хранилища на базе стандартных серверов. Для увеличения их емкости применяют внешние дисковые полки, подключаемые по SAS. Такая система может содержать до сотен дисков на одну СХД. Производительность определяется процессорами, емкостью ОЗУ, типом носителя (HDD/SSD) и пропускной способностью интерфейсов.

Для критичных задач предпочтительнее использовать не просто отказоустойчивый RAID-массив, а двухконтроллерную конфигурацию и дисковые полки с поддержкой «горячей» замены дисков. В случае SDS это два идентичных физических сервера, объединенных в отказоустойчивый кластер (active-active) с синхронизируемой кэш-памятью. При выходе из строя одного узла (контроллера) вся нагрузка переключается на второй. RAID-функции реализуются либо с помощью алгоритмов, задействующих для этих целей ресурсы ЦП, либо с помощью аппаратных RAID-контроллеров или ASIC-устройств.

▲ **Рис. 4.** **Видеосервер Divitec**

Среди SDS-решений можно упомянуть программно определяемую облачную платформу хранения ECS от Dell EMC, которая поддерживает хранение, видеоаналитику неструктурированных данных на обычном оборудовании (типовых серверах). В СХД с программным обеспечением от RAIDIX алгоритмы векторных вычислений призваны гарантировать высокий уровень производительности при последовательных нагрузках. Специфика программной архитектуры и адаптивная система кэширования позволяют СХД одновременно обрабатывать сотни «тяжелых» потоков данных.

Как показывает практика, на базе современных серверных платформ и программных СХД можно успешно строить экономичные хранилища данных для крупных систем видеонаблюдения (до нескольких тысяч камер) емкостью до нескольких петабайт. При этом они будут гарантировать достаточно высокую производительность и отказоустойчивость.

Облачное видеонаблюдение

Видеонаблюдение как сервис на базе облачной инфраструктуры (Video Surveilance as a Service, VSaaS) – одна из актуальных тенденций отрасли, тем более что многие СХД сегодня предлагают интеграцию с сервисами облачного хранения данных. VSaaS представляет интерес для широкой категории заказчиков – от частных пользователей и малого бизнеса до крупных организаций и государственных учреждений. Типичные потребители – розничные сети, строительные организации, небольшие офисы и домохозяйства.

В случае VSaaS видео с камер передается для хранения в ЦОДе провайдера, т.е. по сути это один из вариантов хранения данных в облаке. VSaaS хорошо масштабируется и позволяет наращивать объемы хранимого видео, количество точек наблюдения и число пользователей без значительных капитальных затрат.

В рамках VSaaS чаще всего предоставляется лишь возможность записи и удаленного просмотра видео без какого-либо анализа, но по мере того, как системы видеонаблюдения год от года становятся технически все более совершенными и распространяются все шире, завоевывает популярность облачная «видеоаналитика как сервис». Эксперты предсказывают дальнейший рост этого сегмента. ИКС

Powercom: ИБП без наценки за интеграцию

Об основных тенденциях на российском рынке систем бесперебойного питания рассказывает Григорий Карулин, руководитель направления трехфазных ИБП московского офиса Powercom – компании, которая уже более 30 лет успешно работает на мировом рынке.

– Григорий, какие решения сегодня находятся на технологической передовой в области систем обеспечения бесперебойного электропитания?

– Сейчас самые передовые решения – модульные ИБП, в них вложены основные ресурсы НИОКР ведущих производителей. Почему модульные? Подобная конструкция позволяет минимизировать время ремонта и восстановления, а резервирование на уровне модулей, стоек и параллельных систем повышает уровень отказоустойчивости. Де-факто стандартными для таких ИБП стали единичный коэффициент мощности и КПД на уровне 96%. Эти характеристики снижают совокупную стоимость владения за счет уменьшения тепловых потерь и увеличения плотности мощности на единицу занимаемой площади.

Также хочу отметить гибкость конфигурации модульных ИБП. Если говорить о наших продуктах, то в линейке ИБП Vanguard VGD-M представлены силовые модули на 10, 15, 20, 25, 30, 40 и 50 кВА, из которых можно собирать любые системы мощностью до 1500 кВА. Количество возможных конфигураций исчисляется десятками. Причем модули устанавливаются как в специализированное шасси, так и в стандартную 19-дюймовую стойку. Это удобно, например, для центра обработки данных. Площадь, занимаемая устройством мощностью 300 кВА, составляет 0,66 кв. м, а мощностью 600 кВА – всего 2 кв. м, что позволяет экономить ценное пространство в ЦОДе.

Поскольку денег на нашем рынке немного, даже игроки сегмента high-end проявляют интерес к более дешевым решениям. Как правило, более доступные по цене моноблочные трехфазные ИБП сегодня создаются на базе силовых блоков модульных систем путем урезания части функций. Но, что важно, при этом сохраняются самые высокие показатели и качество флагманских модульных систем. По этому пути пошла и компания Powercom.

Отмечу еще одну тенденцию. Во многих проектах ИБП из ИТ-сегмента перемещаются в ведение поставщиков и монтажников электротехнического оборудования. Речь идет в первую очередь о моноблоках мощностью до 80 кВА. В этих случаях заказчику важна оперативность поставок: сегодня запросил – завтра отгрузили. При этом заказчики стараются сами установить и запустить системы ИБП, сохранив гарантию. Но это, конечно, не ЦОДовские проекты.

– В последнее время разве что ленивый не говорит о «неоспоримых преимуществах» и «огромных перспективах» литий-ионных аккумуляторов. Какова позиция Powercom в этом вопросе?

– Мы видим интерес со стороны заказчиков, получаем соответствующие запросы. Однако расчеты показывают, что существенно более высокий CAPEX делает такие решения экономически не оправданными в сравнении с традиционными свинцово-кислотными аккумуляторами. Даже при 10-летнем горизонте планирования с учетом замены свинцовых аккумуляторов показатель TCO этих решений получается ниже, чем у литий-ионных. Там, где необходимо в компактном объеме и при малом весе получить большое время автономии и сложно обеспечить нужный свинцово-кислотным АКБ температурный режим, конечно, востребованы литий-ионные аккумуляторы. Но в большинстве проектов экономика – это главное, поэтому заказчики предпочитают традиционные АКБ.

– ИБП разных производителей сегодня имеют схожие характеристики. Осталось ли место техническим «фишечкам», которые позволили бы выделиться на общем фоне?

– Силовую электронику (IGBT-транзисторы и пр.) в Китае не выпускают: для всех производителей ИБП ее поставляют всего несколько компаний из Европы, Южной Кореи, Японии и США. ИБП конкурирующих брендов зачастую собираются из одних и тех же компонентов и на одном и том же заводе в Китае. При этом один бренд может быть собственно из Китая, а другой – из Европы или США. Понятно, что качество и базовые характеристики ИБП сегодня примерно одинаковы у большинства ведущих поставщиков.

Но технические «фишки», конечно, остались. Например, Powercom вместо дискретных компонентов в выпрямителе и инверторе ИБП серии VGD-M использует модульные IGBT-транзисторы и тиристоры (six-pack), которые обеспечивают чрезвычайно высокую компактность и надежность устройства в сочетании с высоким КПД. Объединение всех компонентов в одной модульной конструкции исключает дисбаланс технических характеристик компонентов, уменьшает число точек отказа и повышает надежность.

Предлагаемые нами для промышленных применений силовые модули резервного питания имеют уникальное конструктивное исполнение, позволяющее ИБП работать в запыленной окружающей среде. В конструкции ИБП печатные платы и теплоотводы расположены в разных отсеках: поток охлаждающего воздуха проходит через нижний отсек с

Реклама

теплоотводами, не оставляя пыли на печатной плате, которая расположена сверху. Несколько вентиляторов обеспечивают поток воздуха по общему каналу. Если один из вентиляторов выйдет из строя, силовой модуль продолжит свою работу без сбоя в штатном режиме.

Кстати, для промышленных инсталляций Powercom недавно предложила рынку небольшие ИБП серии DRU, монтируемые на стандартную DIN-рейку. Эти устройства, выполненные в компактном дизайне, характеризуются широким диапазоном рабочих температур – вплоть до 50°С – и применяются для обеспечения защиты производственного оборудования: логических контроллеров, средств автоматизации и т.п.

– Такие ИБП можно рассматривать как элементы промышленных edge-ЦОДов?

– Мы не столь сильны в придумывании маркетинговых неологизмов, как некоторые наши конкуренты, но, если хотите, да, это решение для промышленных edge-ЦОДов, можно даже назвать их наноЦОДами.

В целом тема граничных вычислений, edge computing, актуальна для многих заказчиков, поскольку такие решения позволяют обеспечить минимальную задержку при обработке данных и сохранить контроль над важной информацией, не передавая ее в облака. С точки зрения обеспечения бесперебойного электропитания для edge-ЦОДа часто достаточно однофазных систем мощностью 6–10 кВт. Как только используется «трехфазка», надо отводить тепло, ставить кондиционеры.

– А что с энергоэффективностью ИБП? Эта тема выпала из повестки дня?

– Если говорить о работе в режиме онлайн, с двойным преобразованием энергии, то все ведущие производители вышли на уровень КПД 96%. Мы в своем оборудовании реализовали функцию аудита внешней сети. ИБП осуществляет мониторинг параметров на входе. И если, скажем, в течение месяца параметры входного напряжения в норме, то ИБП может перейти в псевдолинейно-интерактивный режим, повысив КПД до 98,5%. Но российские заказчики побаиваются использовать такие «умные» функции. Риски, связанные с переходами из одного режима в другой, для них имеют куда большее значение, чем возможность экономии за счет повышения КПД на пару процентов.

– Действительно, для защиты критичной нагрузки, такой как ИТ-оборудование ЦОДа, заказчику важна надежность и отказоустойчивость. А для этого, в свою очередь, важен профессиональный сервис технического обслуживания ИБП.

– Ну, с этим у Powercom все отлично: больше 150 сервисных центров, которые покрывают всю территорию России, из них 10% работают с трехфазными системами. Вообще, говорить сегодня о серьезном продукте без профессионального сервиса несерьезно.

Есть у нас лаборатория в Москве, где мы можем тестировать оборудование с имитацией условий конкретных проектов. Замечу, что во всех трехфазных ИБП Powercom имеется функция самотестирования, которая позволяет проводить испытания ИБП без реальной нагрузки. Не надо закупать тепловые пушки или другие средства имитации нагрузки, да и электроэнергия экономится существенно – до 90%.

– В области ЦОДов наблюдается тенденция к предложению «из одних рук» комплексных инженерных решений, включающих системы питания, охлаждения, размещения оборудования и управления. У Powercom нет такого комплексного решения. Это осложняет вашу работу?

– Плюсы и минусы комплексных моновендорных решений хорошо известны. Давайте поговорим о преимуществах работы с компанией, которая, как Powercom, специализируется только на ИБП. Это позволяет дополнительно заработать нашим российским партнерам, например, на интеграции различных инженерных подсистем. Крупный вендор, поставляющий такое решение от себя, подобной возможности российских партнеров лишает.

Сегодня многие заказчики стараются взять на себя функции интеграторов, создают собственные центры технической экспертизы. Это связано с сокращением бюджетов, нежеланием платить за интеграторские услуги сторонней организации, которая может необоснованно завышать их стоимость. Но дело не только в этом. Таким образом заказчики получают возможность полностью контролировать проект на всех стадиях его жизненного цикла. Известны же случаи, когда закрываются очень крупные интеграторы, да и зарубежные производители не могут гарантировать, что они не изменят в будущем свое отношение к российскому рынку.

Заказчикам, полагающимся на собственную экспертизу в области инженерной инфраструктуры, выгодно сотрудничать именно со специализированными производителями. Мы, Powercom, обладая многими компетенциями, не навязываем заказчикам свои услуги интеграции, соответственно, не заставляем их оплачивать.

Реклама
PCM POWERCOM
Complete Power Solution™
www.pcm.ru

Российский рынок DWDM: лямбда за лямбдой

Александр Барсков

Технология спектрального уплотнения каналов – «рабочая лошадка», везущая основной груз растущего объема трафика на сетях связи. Она дает возможность повышать пропускную способность сетей без прокладки новых линий и без существенных инвестиций в строительство.

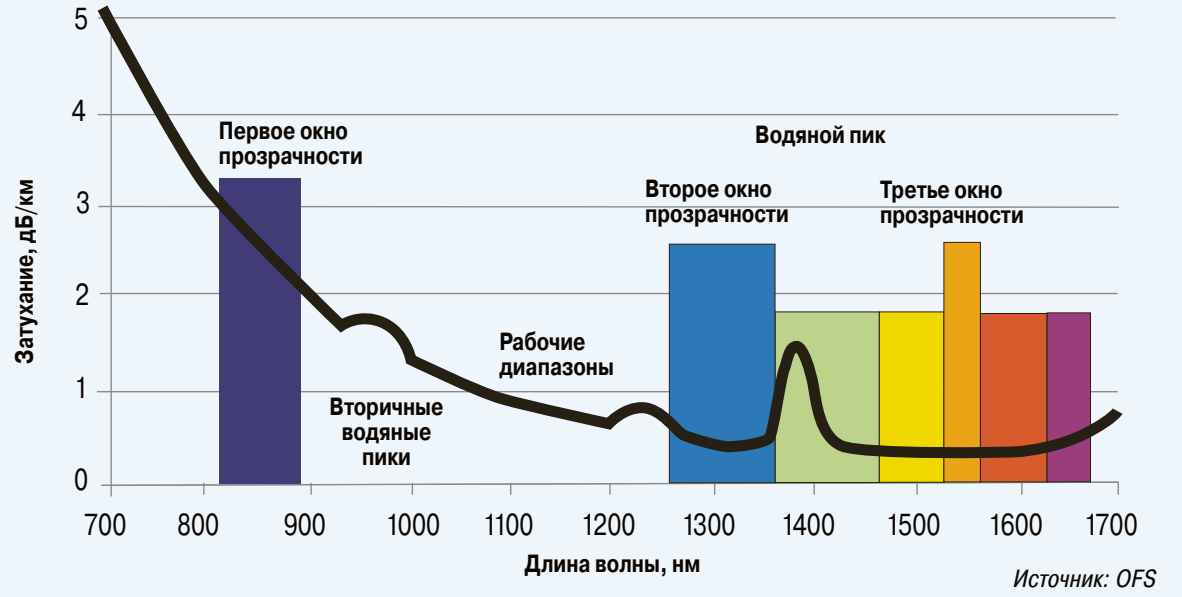
Системы спектрального уплотнения (Wavelength Division Multiplexing, WDM) позволяют передавать по одному оптическому волокну несколько каналов на разных длинах волн. Сегодня активно применяются решения, которые могут «укладывать» в одно волокно до 96 каналов, а пропускная способность каждого канала может достигать 100 или 200G. Таким образом емкость одного волокна составляет терабиты или даже десятки терабит в секунду.

Первые системы WDM были всего лишь двухканальными: с передачей на длинах волн 1310 и 1550 нм (рис. 1). Мощный толчок развитию WDM дало появление в начале 90-х годов прошлого века эрбиевых усилителей, работающих в С-диапазоне (1530–1565 нм), в котором затухание оптического сигнала минимально. Именно в этом диапазоне располагаются спектральные каналы систем DWDM (Dense WDM), причем располагаются очень плотно – типовые решетки имеют шаг 0,4 нм (50 ГГц) или 0,8 нм (100 ГГц), отсюда и слово dense в названии технологии.

Заметим, что наряду с плотным (DWDM) существует и так называемое грубое спектральное уплотнение (Coarse WDM, CWDM). Оно предусматривает передачу в широком диапазоне (1260–1625 нм) до 18 оптических каналов с шагом 20 нм между ними. Большинство каналов систем CWDM не входит в рабочий диапазон длин волн эрбиевых усилителей, поэтому использовать их в этих системах нельзя. В результате область применения решений CWDM ограничивается проектами с небольшими расстояниями между узлами. Пропускная способность таких решений не превышает 10 Гбит/с, а масштабирование – указанных выше 18 каналов.

Российский рынок: ключевые игроки…

На сегодня системы DWDM служат основным транспортом в магистральных сетях национального и трансконтинентального уровня. Достаточно широко эта технология применяется в



Источник: OFS

◀ **Рис. 1.** **Затухание типичного оптического волокна**

региональных сетях. В последнее время отмечается рост ее востребованности в городских сетях, особенно для обеспечения обмена трафиком между центрами обработки данных (Data Center Interconnect, DCI).

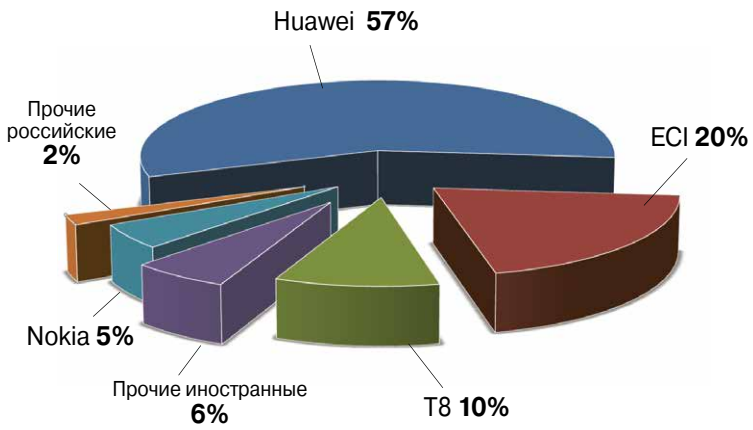
Объем российского рынка оборудования DWDM, оцененный экспертами iKS-Consulting исходя из среднегодового объема заказов на такое оборудование, составил в 2018 г. около $161 млн. Лидером этого рынка с долей в 57% стала китайская компания Huawei (рис. 2). Ее оборудование широко представлено на магистральных сетях «Ростелекома», большой тройки сотовых операторов и «Транстелекома», а в корпоративном сегменте клиентами Huawei являются Банк России, Сбербанк, НСПК, «Связьтранснефть», РЖД, «Автодор» и др.

Также в тройку лидеров по поставкам DWDM-оборудования на российский рынок в 2018 г. вошли израильская ECI (20%) и российская Т8 (10%). Эксперты отмечают существенные колебания объемов продаж у одних и тех же производителей от года к году, что характерно для рынка, на котором один-два крупных проекта могут кратно увеличить продажи. Так, с 2014 по 2017 гг. среднегодовая доля доходов у Nokia была порядка 15%, а компания находилась на втором месте. Однако в результате падения курса рубля и организационных пертурбаций с 2016 г. доходы Nokia на российском рынке, а следовательно, и ее рыночная доля все время снижались, и в 2018 г., по оценке iKS-Consulting, доля компании составила всего 5%. ECI, наоборот, в 2014–2017 гг. не дотягивала до второго места приблизительно три процентных пункта. Но в 2018 г. компания заключила контракты с большой сотовой тройкой и «Ростелекомом» на поставку DWDM-оборудования в рамках выполнения требований «закона Яровой», в результате чего ее доля на российском рынке DWDM-оборудования подскочила до 20%.

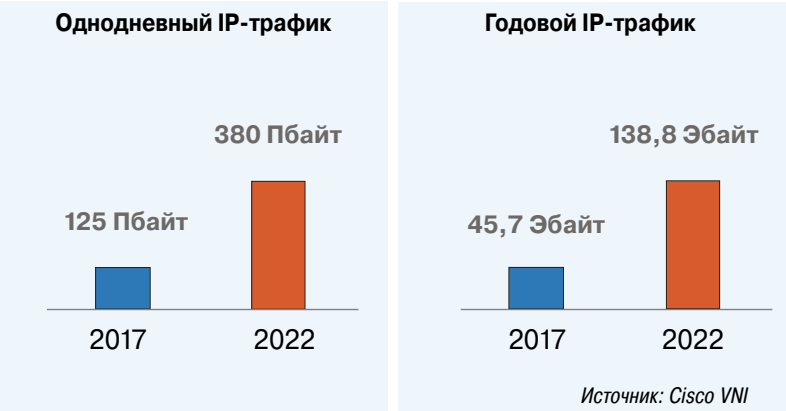
Совокупная доля других зарубежных производителей – PacketLight, Ciena, ADVA, Ekinops, Infinera и Cisco (все они вошли в категорию «Прочие») – в 2018 г. составила приблизительно 6%. Эксперты отмечают существенное снижение показателей этих компаний, тогда как, например, в 2014–2015 гг. Ciena, ADVA и Infinera (вместе с поглощенной в 2018 г. фирмой Coriant) входили в «первый эшелон», каждая в отдельности занимая более 5% российского рынка.

Помимо Т8 – явного лидера среди отечественных производителей оборудования DWDM – в России работают еще несколько компаний, чью продукцию в большей или меньшей степени можно признать отечественной, но их суммарная доля в 2018 г. составила всего 2%. Это, в частности, питерская «Супертел», оборудованию которой, как и продукции Т8, присвоен статус ТОРП – телекоммуникационного оборудования российского производства. Выпуск DWDM-обо-

Рис. 2. **Доли крупнейших поставщиков DWDM-оборудования в России в 2018 г.** ▼



Источник: iKS-Consulting



▲ Рис. 3. Прогноз роста IP-трафика в России в 2017–2022 гг.

рудования не главный вид деятельности данного предприятия, поэтому если общая среднегодовая выручка «Супертел» и Т8 за предыдущие пять лет сравнимы, то по доле доходов от продаж DWDM-оборудования петербургский изготовитель существенно уступает Т8. На рынке присутствуют и еще два российских производителя DWDM-оборудования. Это НТО «ИРЭ-Полюс», дочерняя компания международного концерна IPG Photonics, и компания Qtech, выпускающая различное телекоммуникационное оборудование, в том числе «коробочные» DWDM-устройства для региональных и городских сетей связи.

Российские производители DWDM-оборудования пытаются конкурировать с иностранными поставщиками, совершенствуя функциональные возможности, наиболее востребованные на российском рынке. Но у них отсутствует собственная электронная компонентная база, а скромные бюджеты на НИОКР не идут ни в какое сравнение с теми, что имеются в распоряжении мировых грандов. Так что о серьезной конкуренции с глобальными лидерами рынка DWDM-оборудования в сфере новейших научно-технических достижений говорить не приходится.

Мультисервисная DWDM-платформа «Волга» российского производства ▶

Политика импортозамещения вкупе с международными санкциями, с одной стороны, способствует росту продаж отечественного оборудования DWDM, а с другой – несет угрозу еще большего технологического отставания, поскольку многие комплектующие для систем DWDM приобретаются за рубежом, в том числе у американских компаний.

…и ключевые заказчики

Крупнейшим потребителем DWDM-оборудования в России является компания «Ростелеком», которая в период 2014–2018 гг. закупала это оборудование в среднем на $30 млн в год. Далее следует большая сотовая тройка – «Мегафон», МТС и «Вымпелком», – а замыкает топ-5 основных заказчиков ТТК. По оценке iKS-Consulting, объем среднегодовых заказов первой пятерки российских потребителей составлял в 2014–2018 гг. примерно 57% среднегодового объема всего российского рынка DWDM-оборудования. Совокупные среднегодовые закупки операторов регионального уровня в этот период iKS-Consulting оценивает цифрой, почти вдвое меньшей объема закупок первой пятерки, хотя численность игроков этого сегмента на порядок больше.

Среди представителей корпоративного сектора, активно использующих DWDM, аналитики выделяют банковские структуры (в первую очередь Сбербанк), предприятия энергетического, нефтегазового и транспортного секторов. В частности, «Транснефть» задействует DWDM при строительстве сети вдоль нефтепровода «Сила Сибири», «Автодор» – вдоль трассы Москва – Санкт-Петербург, а РЖД – вдоль московской кольцевой железной дороги с хордами и заходами в Москву. Предприятия энергетики в лице своих корпоративных операторов связи, например «Иркутскэнергосвязь», внедряют DWDM на сетях технологической связи.

Следует выделить использование DWDM для подключения и организации каналов связи между ЦОДами. В решениях DCI, как правило, применяются наиболее современные технологии. В частности, каждый спектральный канал (лямбда) обеспечивает передачу 100 Гбит/с, тогда как в промышленных сетях зачастую устанавливается более дешевое оборудование со скоростями 10 Гбит/с на лямбду. Основные заказчики решений DCI в России – это крупные финансовые структуры.

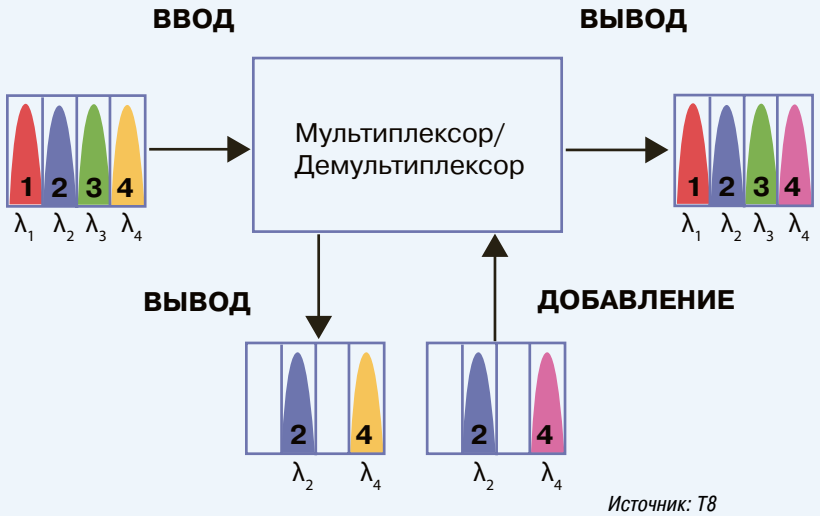
Анатомия роста

Главный драйвер спроса на оборудование DWDM – рост трафика, который, по всем прогнозам, продолжится (рис. 3). По мнению Евге-

Что такое ROADM

Реконфигурируемый мультиплексор ROADM позволяет программно изменять распределение спектральных каналов по волокнам. В основе такого мультиплексора – матрица селективного переключения спектральных каналов (Wavelength Selective Switch, WSS), которая способна направить пришедший на входной порт спектральный канал (лямбду) на любой из N выходов.

Принцип работы мультиплексора ROADM



Источник: Т8

ния Жукова, отвечающего в компании Huawei за решения для операторов связи, этот рост будет связан с передачей данных облачных услуг, видеоконтента, с обменом данными между ЦОДами, развитием сетей 5G, интерактивных приложений, систем виртуальной и дополненной реальности (VR/AR). «Все это будет стимулировать переход в магистральных сетях на 200G- и 400G-лямбды», – считает эксперт Huawei.

Влияние 5G – наиболее горячая тема в телекоммуникационном мире – на увеличение объемов трафика и соответственно спроса на системы DWDM проявится не в этом году. «Через два года можно ожидать нового всплеска масштабной модернизации DWDM-сетей, который будет связан с подготовкой к вводу в эксплуатацию сетей 5G», – прогнозирует Леон Тылевич, президент регионального подразделения ECI Telecom по России и СНГ.

Операторы ожидают, что с вводом в строй сетей 5G основной трафик будут генерировать не частные пользователи, а миллионы подключенных устройств (датчики, счетчики и т.д.), которые будут передавать информацию в различные ЦОДы. Развитие IoT вызовет и увеличение видеотрафика – например, при срабатывании датчика открытия ворот пользователь захочет посмотреть, кто собирается в них заехать, соответственно, по сети пойдет видео, причем в высоком разрешении.

Но и связываемый с развертыванием сетей 5G бум роста IoT-трафика – дело не сегодняшнего дня. «Чтобы IoT начал "давить" на транспортную сеть, нужно, чтобы в IoT-сетях были сотни тысяч устройств. Это произойдет никак не раньше 2021–2022 гг.», – дает свою оценку Константин Лукин, генеральный директор компании «Супертел».

Операторы связи рассчитывают на серьезное увеличение объемов трафика, передаваемых через Россию транзитом. «Мы надеемся на увеличение (числа) каналов в Европу из Китая и Японии, а после построения Южного кольца – и из Индии», – говорит Николай Кастомаров из «Трансителекома». Он отмечает, что в Китае и Индии бурно идут процессы цифровизации. Так, известно, что многие международные компании размещают свои колл-центры в Бангалоре, откуда идет огромный поток трафика.

Помимо возможности нарастить пропускную способность оптических каналов связи без прокладки нового волокна важным фактором, определяющим интерес заказчиков к решениям DWDM, является возможность организовать канал оперативно. «Если у вас уже есть оптический кабель и вам нужен дополнительный канал, то с помощью DWDM-оборудования за несколько часов можно организовать 80 дополнительных каналов на том же самом волокне. Эта оперативность перекрывает все остальное. У меня есть опыт создания нового канала 10 Гбит/с Петербург – Вологда в течение четырех часов. Никакая другая технология не позволяет получить новый канал связи так быстро», – делится опытом Константин Марченко, заместитель генерального директора Т8.

Эксперт Т8 также отмечает, что с повышением доступности спектральных каналов клиенты стали чаще брать «под каждый сервис отдельную лямбду». «Естественно, у разных сервисов разные требования к пропускной способности, и далеко не каждому необходим канал 100G, тем более 200G или 400G. Но важно, что спектральный канал обеспечивает физически отдельную среду передачи. У клиентов есть несколько функциональных систем, и они не хотят, чтобы эти системы влияли друг на друга,

поэтому стремятся их разнести по разным лямбдам», – продолжает он.

При увеличении числа спектральных каналов, в том числе за счет использования отдельного канала для каждого сервиса, все более востребованной на рынке будет их коммутация. Такой функционал реализуют реконфигурируемые оптические мультиплексоры ввода-вывода (Reconfigurable Optical Add/Drop Multiplexer, ROADM) – относительно новый класс оборудования, которое в России пока применяется очень ограниченно. Мультиплексоры ROADM устанавливают, как правило, крупные операторы и богатые структуры, например, Сбербанк. Но даже у таких потребителей ROADM, по оценке iKS-Consulting, затрагивают менее 10% лямбд.

Ценовой барьер

Цена на DWDM-оборудование постепенно снижается, но, как указывают операторы, медленнее, чем тарифы на пропуск трафика. Таким образом, динамика снижения стоимости DWDM-оборудования не компенсирует потери от падения тарифов. Это вынуждает операторов, особенно не крупных, приобретать более дешевое оборудование, что расширяет ниши, в частности, российских производителей.

Одна из тенденций, которую отмечают аналитики, – это уменьшение стоимости сетевого оборудования за счет замены активных компонентов на пассивные. Для российского рынка этот фактор очень важен, так как многие операторы и владельцы ЦОДов регионального и городского уровней, органы региональной и городской власти, а также представители не самого крупного бизнеса не могут позволить себе наивысшие достижения в области DWDM.

В ожидании бурного роста

Уровень развития телекоммуникационной инфраструктуры в нашей стране можно считать вполне удовлетворительным, особенно с учетом огромных расстояний и относительно низкой плотности населения. В России построена разветвленная оптическая сеть с множественным резервированием маршрутов, охватывающая практически всю территорию страны с запада на восток. Пропускная способность сети на направлении Москва – Санкт-Петербург превышает 60 Тбит/с, Москва – Хабаровск – 10 Тбит/с, а еще на восьми направлениях – 2 Тбит/с (подробнее см. Г. Башилов. Связность российских ЦОДов: вперед, в регионы? «ИКС» № 3'2019, с. 56).

Основные маршруты магистральных сетей РФ были сформированы уже к середине 10-х годов. С тех пор их пропускная способность наращивалась путем замены активного оборудования, обеспечивавшей переход с 10- и/или 40-гигабитных оптических каналов на 100-гигабитные. По мнению экспертов iKS-Consulting, в ближайшие несколько лет бурного строительства сетей не предвидится, а необходимое увеличение пропускной способности будет достигаться главным образом умощнением существующих сетей с помощью технологии DWDM.

Там, где на федеральных магистралях ключевыми потребителями DWDM-оборудования («Ростелеком», большая тройка и ТТК) установлено когерентное оборудование, будет постепенно увеличиваться число спектральных каналов 100G и 200G. На региональных магистралях будет наблюдаться переход с каналов 10G на 100G, а в региональных сетях агрегации трафика – рост числа каналов 10G.

Строительство новых магистралей возможно в ближайшие годы вдоль автомобильных трасс от Хабаровска до границы с Беларусью («Автодор»), а также в рамках реализации цифрового Шелкового пути от границы Казахстана также до Беларуси. Как известно, еще в начале 2019 г. «Транснефть Телеком» сообщила о своей победе в тендере China Unicom Global на прокладку транзитного канала связи емкостью 100 Гбит/с на участке Китай – Европа через территории Казахстана, России и Беларуси.

Важным стимулом для развития инфраструктуры связи может стать рост центров хранения и обработки данных, а также все более активное использование корпоративными заказчиками облачных сервисов. Однако и в этой, в целом динамично развивающейся области, есть определенные проблемы. Так, по данным iKS-Consulting, 2019 г. стал третьим годом подряд, в котором рост емкости ЦОДов на территории РФ замедлялся. В 2019 г. количество дата-стоек в России, по предварительным данным, выросло всего на 9,4%, тогда как в предыдущем году этот показатель составил 10,8%, а в 2017 г. – 13%. Кроме того, в последние два года емкость дата-центров стабильно увеличивается лишь за счет Москвы и области, где мощность DWDM-сетей и так уже достаточно высока.

Эксперты ожидают, что в текущем году начнется активное строительство дата-центров в регионах и это подхлестнет развитие сетей связи для их подключения и организации межЦОДовского взаимодействия. Кроме того, в 2022 г. можно ожидать нового всплеска масштабной модернизации DWDM-сетей, который будет связан с подготовкой к вводу в эксплуатацию сетей 5G. Но в целом, по прогнозу iKS-Consulting, в ближайшие четыре года рынок DWDM-оборудования в России будет расти примерно на 6% за год. ИКС

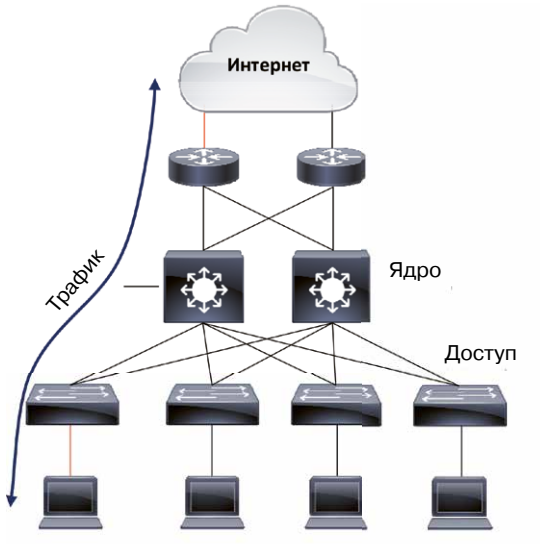
Какой должна быть сетевая фабрика ЦОДа

Одной из важных задач при проектировании центра обработки данных является выбор сетевого оборудования: при недостаточной функциональности страдает качество сервисов, а при избыточной неоправданно увеличивается их стоимость.

Михаил Антошкин, старший инженер, «ЛАНИТ-Интеграция» (ГК ЛАНИТ)

Разворачивая потоки трафика

Сетевое оборудование выбирается исходя из планируемых нагрузок и архитектуры сети, в которой оно будет работать. Для современной корпоративной сети нагрузку составляют преимущественно небольшие потоки трафика от пользователей, и направлены они «с юга на север», т.е. от коммутаторов доступа к пограничным маршрутизаторам (рис. 1).



▲ **Рис. 1. Основные направления трафика в типичной корпоративной сети**

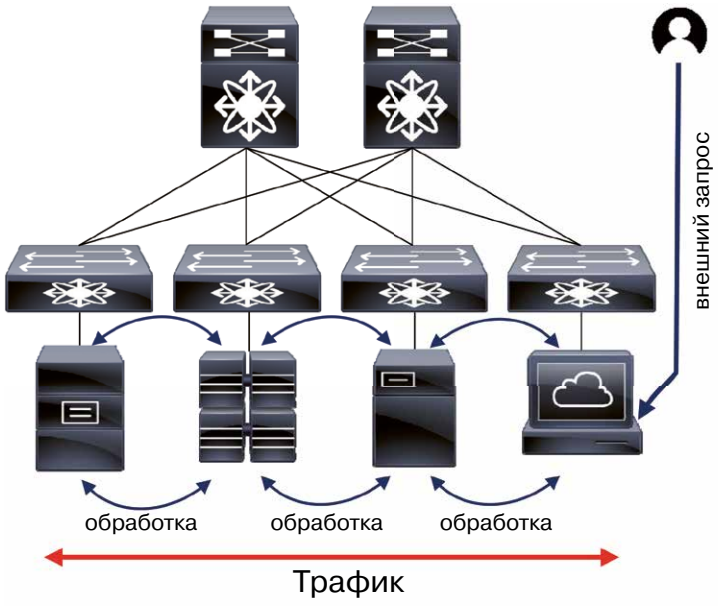
Высокая скорость внутри сети здесь востребована мало – все равно ее ограничит «бутылочное горлышко» в виде пропускной способности внешних каналов. Да и ситуации, когда пользователь создает нагрузку на сеть даже в 100 Мбит/с, довольно редки и продолжаются недолго.

В сети центра обработки данных ситуация иная. Основной объем трафика здесь идет «с востока на запад», т.е. между коммутаторами внутри сети (рис. 2), и объем его значительно больше. Главная причина такого характера трафика – в архитектуре приложений, которые обычно разворачиваются на оборудовании, размещенном в ЦОДе.

К примеру, пользователь зашел на сайт, хостинг которого обеспечивает ЦОД, – это всего один внешний запрос от пользователя к веб-серверу. Но внутри ЦОДа он создал целый набор подключений: от балансировщика нагрузки к front-end-серверу, от него к серверу back-end, от того к базе данных и обратно. При этом каждое соединение – дополнительная задержка для пользователя, который ждет свою веб-страницу.

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

Рис. 2. Основные направления трафика в сети ЦОДа ▼



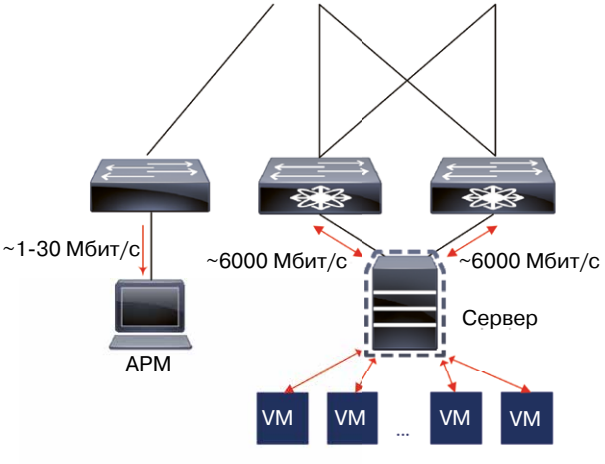


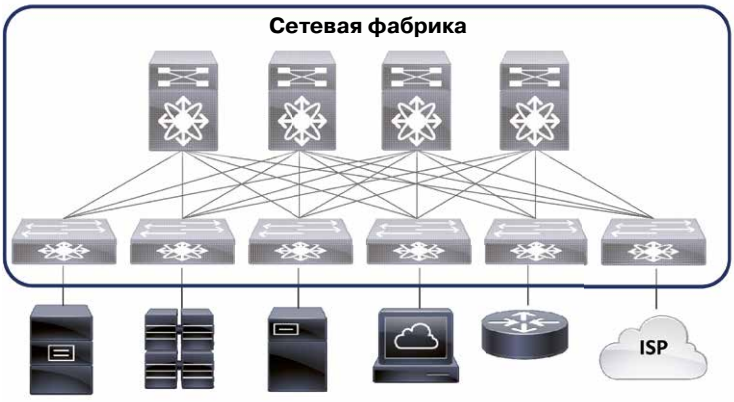
Рис. 3. ▶ **Примеры скоростей передачи данных в корпоративной сети (слева) и в сети ЦОДа**

перемещаться, значит, широкая полоса пропускания необходима везде (рис. 3).

Ключевые устройства в сети ЦОДа – это коммутаторы, которые являются самым эффективным по стоимости 1 Гбит/с сетевым компонентом, способным обеспечить нужную производительность.

Потоки трафика, которые не покинут сеть ЦОДа и не требуют инспекции с помощью ИБ-оборудования, обычно обрабатываются исключительно коммутаторами. Группу коммутаторов, которые доставляют такой трафик в пределах одного ЦОДа, обычно выделяют в особую логическую единицу и называют ее сетевой фабрикой (рис. 4).

Рис. 4. **Сетевая фабрика в ЦОДе** ▼



Помимо необходимости обеспечить высокую пропускную способность архитектуру сетевой фабрики определяют требования к отказоустойчивости. В корпоративной сети отказ коммутатора доступа обычно означает только то, что подключенная к нему группа пользователей временно не сможет работать. Да и полностью защититься от его отказа невозможно – у пользовательского компьютера только один сетевой интерфейс, больше чем к одному коммутатору его не подключишь.

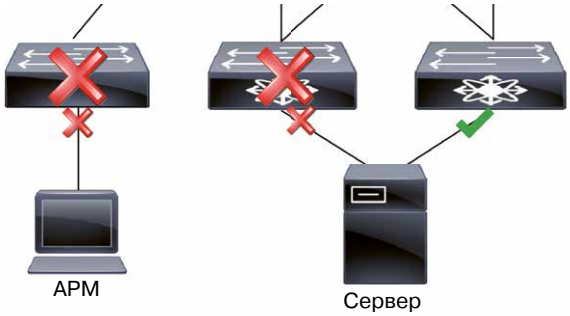


Рис. 5. **Резервирование в сети ЦОДа (справа) и отсутствие резервирования подключения конечных устройств в типовой корпоративной сети** ▶

В ЦОДе же такое недопустимо. Если доступ к сети потеряет даже один сервер, то это может причинить ущерб вплоть до остановки бизнес-процессов целой компании – все зависит от критичности приложений, которые на этом сервере размещены. Поэтому в сети ЦОДа резервируется всё, начиная с подключения конечных устройств, коммутаторов и до подключения ЦОДа к внешним сетям (рис. 5).

«Дерево» сети ЦОДа

Архитектура сетевой фабрики воплощает простой принцип – максимально быстрая и резервированная связь между любыми двумя коммутаторами. Он реализуется в сети Клоза. В ней коммутаторы могут играть всего две роли: «листьев» (Leaf), к которым подключаются серверы и внешние сети, и «ствола» (Spine), который обеспечивает взаимодействие «листьев» (рис. 6).

Использование такой архитектуры в ЦОДе дает ряд преимуществ по сравнению с классической двухуровневой архитектурой со «свернутым» ядром сети (collapsed core):

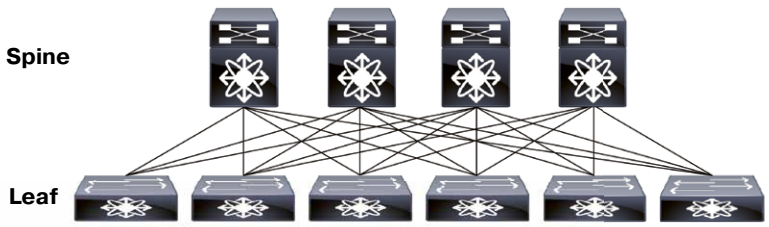
- Увеличивается отказоустойчивость. В сети collapsed core независимых ядер может быть только два – это ограничение технологий агрегации MLAG (Multi-Chassis Link Aggregation), которые позволяют объединять интерфейсы в группы максимум между двумя коммутаторами. Коммутаторов же Spine может быть гораздо больше.
- Легче увеличивать пропускную способность – для этого нужно просто добавить необходимое число коммутаторов Spine.
- Сбои затрагивают меньше устройств – коммутаторы полностью независимы, отказоустойчивость достигается без использования стекирования или MLAG.
- Задержка становится предсказуемой – на пути любого потока внутреннего трафика находится только один коммутатор Spine.
- Повышается уровень утилизации сетевых интерфейсов – трафик между Leaf и Spine прозрачно и эффективно распределяется с помощью механизмов ECMP (Equal Cost Multipath).

Самое очевидное требование к коммутаторам в сетевой фабрике – наличие нужного количества портов с определенной скоростью. Фактически именно оно определяет производительность фабрики. Выбор заказчиками оборудования это практически не ограничивает – сейчас у большинства вендоров есть модели со скоростями интер-

фейсов от 1 до 400 Гбит/с. При этом для различных типов нагрузки хорошо подходят модели с определенным дополнительным функционалом.

Разные особенности сетевых фабрик

Если фабрику предполагается использовать как транспорт для СХД, то стоит обратить внимание на коммутаторы с глубоким буфером. Многие протоколы доставки данных критически реагируют на потерю пакетов – либо останавливают передачу данных, либо существенно ее замедляют. При этом в ряде случаев увеличение скоростей на эту ситуацию не повлияет: скажем, когда одна из сторон данные отправляет, а другая принять их не готова (например, перегружена запросами). Глубокий буфер (у некоторых производителей его размер достигает 1 Гбайт) позволяет коммутаторам буферизовать такие «лишние» данные и при наличии у серверов/СХД механизмов управления скоростью передачи данных практически полностью избежать потерь пакетов (рис. 7).



▲ Рис. 6. Архитектура Leaf – Spine

Если планируется использовать стороннюю, полностью программную систему виртуализации сети, то полноценная поддержка VXLAN EVPN на коммутаторах обычно не требуется, они предоставляют системе виртуализации простую L3-связность. В таком случае может быть достаточно поддержки на коммутаторе простого VXLAN-туннелирования в сочетании с протоколом OVSDB (Open vSwitch Database Management Protocol). OVSDB позволяет частично отдать коммутатор под управление контроллеру системы виртуализации сети для того, чтобы он мог распространить действие политик виртуальной сети на физические серверы, а VXLAN дает возможность эту виртуальную сеть «дотянуть» до них.

◀ Рис. 7. Логика работы механизма управления скоростью передачи

Для наиболее эффективной работы фабрики взаимодействие между коммутаторами должно происходить на третьем (сетевом) уровне модели OSI. Но архитектура приложений может потребовать взаимодействия на втором (канальном) уровне, а если ЦОДов и фабрик несколько, может возникнуть необходимость растянуть между ними эти широковещательные сегменты (часто встречающийся пример – VMware VMotion, один из способов обеспечить отказоустойчивость виртуальных машин с сохранением адресации). В таких случаях стоит рассмотреть коммутаторы с поддержкой технологий виртуализации сети.

Довольно популярный и широко поддерживаемый производителями вариант – VXLAN (Virtual Extensible LAN) в сочетании с EVPN (Ethernet Virtual Private Network). VXLAN туннелирует трафик второго уровня в пакеты UDP, а EVPN контролирует процессы построения VXLAN-туннелей и распространения информации о MAC-адресах между коммутаторами. Ключевая особенность использования информации о MAC в EVPN заключается в том, что такой адрес привязывается не к физическому порту, а к IP-адресу коммутатора, на котором этот MAC находится.

Если от фабрики требуется нетиповой функционал, не реализованный ни одним из вендоров, к примеру, сложная балансировка трафика или его маршрутизация/коммутация/фильтрация на основе нестандартных признаков, то хорошим выбором может стать использование коммутаторов с программируемыми ASIC. Они позволяют описать логику обработки трафика на специальном языке программирования, после чего коммутатор сможет выполнять ее практически со скоростью сетевых интерфейсов. К сожалению, на данный момент при работе в таком режиме коммутаторы требуют заново описать и всю стандартную логику (включая классические протоколы маршрутизации), но производители работают над выпуском «комбинированных» устройств.

Итак, при выборе сетевого оборудования необходимо ориентироваться на специфику конкретной задачи. На рынке представлен достаточно широкий ассортимент продуктов, и всегда можно выбрать решение, которое обеспечит требуемые современному ЦОДу производительность и функциональность сетевой инфраструктуры ИКС

Kehua в России: удвоение каждый год

Kehua – бренд ИБП, представленный в нашей стране с 2018 г. Продвигает его один из старожилов рынка – компания «Абсолютные Технологии». О первых итогах сотрудничества и его перспективах рассказывает коммерческий директор этой компании Вячеслав Бурлаков.

– Вячеслав, давайте начнем с реализованных проектов. О каких успехах можете рассказать?

– В 2019 г. у нас появилось немало проектов, которые мы называем референсными. Зачастую они реализуются с минимальной маржинальностью, но закладывают перспективы многолетнего сотрудничества и тиражирования решений в разных отраслях. Такие проекты идут в госорганизациях, промышленности, медицине, финансах, телекоме, ИТ и т.д.

Например, для нашего стратегического партнера РЖД в декабре 2019 г. завершили проект поставки ИБП для МЦД. Оборудование Kehua обеспечивает на станциях бесперебойное электропитание систем аварийного освещения, видеонаблюдения и т.п. Еще один оснащенный нами объект – стадион «Локомотив», где реализована комплексная система бесперебойного и гарантированного электропитания, включающая ИБП и дизель-генераторные установки.

Сегодня мы ведем много проектов в медицине. Компания «Абсолютные Технологии» – основной поставщик ИБП для медицинских систем Canon Medical. Мы успешно работаем с медицинскими подразделениями Philips и Siemens. ИБП Kehua устанавливаются для многих диагностических комплексов, в том числе в рамках национальной онкологической программы. В таких комплексах требования к ИБП очень высоки.

Большой задел у нас и для работы в сферах ИКТ, дата-центров, включая все более востребованные модульные ЦОДы. В частности, ИБП Kehua используются в модульных ЦОДах, поставляемых нашим партнером российской компанией GreenMDC. Сейчас выполняется ряд крупных проектов систем электропитания ЦОДов для разных заказчиков, в том числе банков.

– Ваш партнер – китайский производитель. Какие преимущества дает то обстоятельство, что это именно компания из Поднебесной?

– Во-первых, мы получаем очевидное технико-экономическое преимущество: современные технические решения мирового лидера рынка трехфазных систем бесперебойного электропитания при относительно невысокой стоимости изделия. Оборудование Kehua имеет хорошие технические данные, высокое качество сборки, широкий спектр опций, что позволяет с легкостью конкурировать с европейскими вендорами.

Во-вторых, Россия и Китай – стратегические партнеры. Это снимает санкционные риски. Мир быстро и зачастую непредсказуемо меняется. Многие заказчики, перед которыми встает задача замены ИБП, все чаще задаются вопросами, что будет завтра с поддержкой и модернизацией выбираемых технических решений, как изменится работа в России именитых западных брендов.

Одна из тенденций – стремление заказчиков заключать контракты полного жизненного цикла, которые рассчитаны, скажем, на 10 лет. И здесь ценно наличие стратегического партнера, которое минимизирует риски.

– Для критичных систем важны надежность и качество ИБП. Здесь проблем не возникает?

– Мы долго выбирали партнера. Досконально изучали оборудование Kehua, тщательно тестировали. Собирали и анализировали отзывы заказчиков. Некоторые компании эксплуатируют ИБП Kehua с 2018 г., и никаких проблем или сбоев в работе, повлекших отключение или сбой в ответственной нагрузке, зафиксировано не было.

Нужно понимать, что надежность любого решения складывается из двух основных компонентов: надежности самой техники и квалификации и опыта специалистов. Сейчас в индустрии ЦОДов все больше внимания уделяется обучению персонала. Ведь, по статистике, значительная часть проблем связана именно с человеческим фактором. Поэтому всех, кому мы передаем право обслуживать оборудование Kehua, стараемся хорошо обучить.

– Kehua – относительно новое имя на высококонкурентном рынке ИБП. И уже много проектов. В чем причина успеха?

– «Абсолютные Технологии» не первый год на рынке, нас знают, нам доверяют оснащение самых важных систем. За 20 лет мы собрали команду специалистов, которая способна реализовать любое сложное решение. Ну а широкий спектр оборудования Kehua позволяет закрывать все потребности – от малых ИБП для серверных до самых мощных систем для мегаЦОДов и промышленных предприятий.

Заказчики, особенно крупные, ценят возможность тестирования и опытной эксплуатации оборудования на объекте. Мы такую возможность предоставляем. Кроме того, у нас есть свой комплект оборудования и необходимое ПО для проверки ИБП и моделирования нагрузки, специфичной для конкретного объекта. Мы вместе с заказчиками проверяем ИБП в условиях, максимально приближенных к «боевым».

ЦОДы тоже стремятся потрогать выбираемое оборудование, протестировать его. Например, сейчас мы реализуем

Реклама

проект ЦОДа для одного из коммерческих банков. Встала задача замены ИБП, выработавших свой ресурс. Прежде всего специалисты банка провели физические испытания, тесты с перегрузкой, детально изучили механическую конструкцию ИБП, компоновку плат, качество лакового покрытия и т.д. Только после этого нас допустили к участию в тендере, в котором мы и победили.

Большой плюс работы с Kehua в том, что завод прислушивается к запросам российских заказчиков. Один из примеров – потребность российских компаний в ИБП с увеличенным временем автономной работы от аккумуляторных батарей. Речь идет о системах относительно небольшой мощности, которые востребованы в edge-решениях. Специалисты Kehua оперативно решили задачу: предложили модели ИБП с увеличенным зарядным током и возможностью подключения внешней АКБ большой емкости, способные обеспечить до нескольких часов автономной работы.

– Вы затронули быстро развивающийся сегмент edge-ЦОДов. Какие системы электропитания устанавливаются на таких объектах?

– Среднее энергопотребление микро- и мини-ЦОДов 30–40 кВт. При этом, как уже говорилось, важна возможность увеличенного времени автономии, поскольку edge-ЦОДы часто размещаются на большом удалении от сервисных центров, в труднодоступных местах и пр.

Есть хорошие решения на традиционных свинцово-кислотных АКБ. Безусловно, большие перспективы у ИБП с литий-ионными аккумуляторами. У таких АКБ множество преимуществ: они позволяют уменьшить занимаемые площади, снизить расходы на кондиционирование, поскольку не предъявляют столь жестких требований к температуре эксплуатации, как свинцово-кислотные.

В отличие от большинства конкурентов, Kehua использует литий-ионные АКБ, разработанные с одним из партнеров специально для ИБП, а технология LFP обеспечивает более высокий уровень безопасности при повышении температуры.

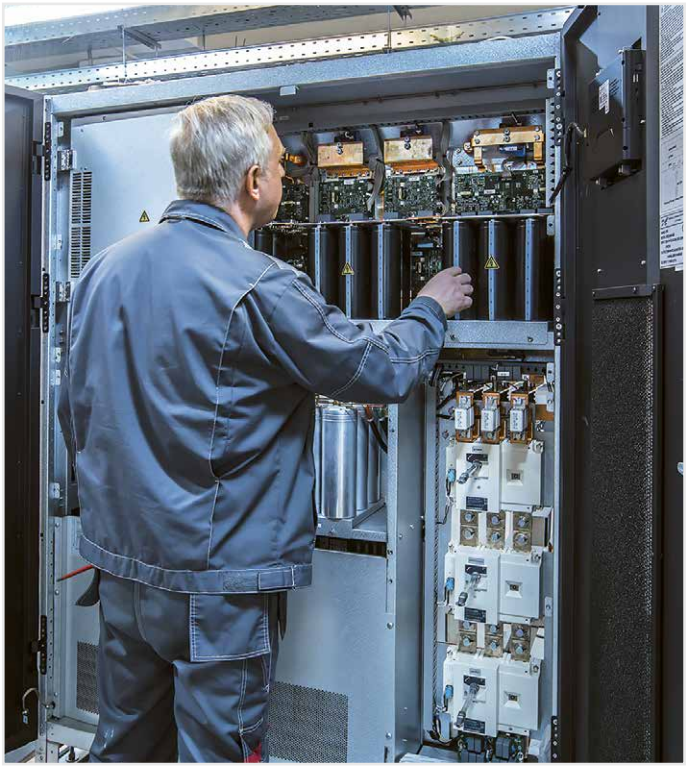
– Edge-ЦОДы все чаще разворачивают в промышленности. Что вы предлагаете для этого сегмента?

– У Kehua есть промышленные ИБП. Это системы с повышенным уровнем защиты, с дублированием плат управления, систем охлаждения. Данные серии рассчитаны на работу в неблагоприятных условиях, в средах с повышенным содержанием пыли и влаги, с соляным туманом. Такие ИБП поставляются и российским заказчикам. В частности, ИБП Kehua устанавливаются в комплексах Honeywell – одного из крупнейших производителей оборудования и прикладного ПО в области промышленной автоматизации.

– Другое направление ускоренного роста – крупные (мега-, гипер-) ЦОДы. Такие объекты появляются и в России. Какие решения предлагаете для них?

– Компания Kehua, что весьма необычно для производителя оборудования, самостоятельно построила и эксплуатирует несколько ЦОДов, к услугам которых прибегают такие гиганты рынка, как Alibaba, Baidu и Tencent. Мощность дата-центров достигает 32 МВт. Мы стараемся использовать богатый опыт и экспертизу Kehua для строительства ЦОДов в России.

У китайских компаний амбициозные планы расширения присутствия на российском рынке ЦОДов. В Китае Kehua для



них – главный партнер в части ИБП. Надеемся, что благодаря этому оборудование Kehua будет задействовано и при реализации проектов крупных китайских компаний в нашей стране.

Когда говорят о гиперЦОДах в России, как правило, имеют в виду объект «Росэнергоатома» в Удомле. У этой корпорации большие планы строительства новых дата-центров, и мы активно с ней сотрудничаем. Причем в новых мегаЦОДах, в отличие от объекта в Удомле, скорее всего будут устанавливаться не динамические, а статические ИБП. На помощь нам как поставщику статических ИБП пришли уже упоминавшиеся литий-ионные АКБ. Использование статических ИБП с литий-ионными батареями позволяет получить компактные решения, сравнимые по занимаемой площади с динамическими ИБП.

У Kehua есть системы ИБП мощностью до 4,8 МВт. По нашим оценкам, с учетом снижения цен на литий-ионные АКБ при горизонте планирования 10 лет такие решения получаются выгоднее динамических ИБП.

– Год назад Kehua и «Абсолютные Технологии» заявили о намерении в течение ближайших трех лет занять до 10% российского рынка ИБП. Как вы продвигаетесь к этой цели?

– С оборудованием Kehua мы плотно работаем уже два года. В 2019 г. объем продаж и в натуральном, и в денежном выражении вырос примерно в два раза. Планы на этот год не менее амбициозные. С учетом созданной базы референсных проектов объем поставляемого оборудования Kehua планируем также увеличить вдвое.

акционерное общество
АБСОЛЮТНЫЕ ТЕХНОЛОГИИ
www.absolutech.ru

Реклама

Как улучшить оптические соединители?

Андрей Семенов, профессор, МТУСИ

Современные разъемные волоконно-оптические соединители при соблюдении правил их эксплуатации обеспечивают затухание столь малое, что его дальнейшее снижение сопряжено с большими техническими сложностями, а выигрыш практически не сказывается на характеристиках линии связи.

Так, швейцарская компания Diamond FO еще в середине 2000-х годов полностью отработала технологию активной юстировки, позволяющую даже для одномодовых изделий гарантировать вносимые потери на уровне 0,05 дБ, но развития эта технология не получила.

В итоге усилия по совершенствованию соединителей, как многоканальных, так и дуплексных, были сосредоточены на том, чтобы сделать их более удобными в использовании для персонала, непосредственно работающего с волоконно-оптической техникой.

Внедрение дуплексных конструкций в 400-гигабитные тракты

Одна из проблем магистральных сетей связи – так называемый скоростной предел электроники: быстродействие схем обработки данных заведомо ниже требуемой скорости передачи. Применение блочных и многоуровневых кодов для уменьшения тактовой частоты лишь отчасти снимает остроту проблемы. Эффективным же является переход на параллельную передачу, т.е. разбиение сообщения на несколько частей, каждая из которых передается в своем субканале с меньшей скоростью, а затем восстановление исходного сообщения на приеме.

Оптическая подсистема ЦОДов, в отличие от сетей связи общего пользования, из соображений минимизации стоимости в подавляющем большинстве случаев строится на многомодовой элементной базе, что позволяет реализовать параллельную передачу одним из двух способов. Первый – пространственное уплотнение – подразумевает, что каждому субканалу ставится в соответствие свое волокно. Количество световодов при этом варьируется от 8 до 24. В последнее время в силу разных причин отрасль тяготеет к схеме Base 8 (четыре волокна на прием и четыре на передачу). Второй способ – использование четырехканального коротковолнового спектрального уплотнения SWDM – выгоден тем, что для скоростей вплоть до 200 Гбит/с дает возможность сохранить удобную в эксплуатации двухволоконную структуру тракта и не отказываться от применения стандартного соединителя LC.

Однако на скоростях 400 Гбит/с, которые, как ожидается, будут массово востребованы в ЦОДах уже к середине следующего десятилетия, физическая параллельная передача пока безальтернативна. Создание группового разъема на базе LC вполне возможно технически. Одно из решений доведено до уровня предложений консорциума производителей активного сетевого оборудования и базируется на горизонтальной сборке вилок этих разъемов, но оно невыгодно из-за больших габаритов.

Таким образом, бесшовный переход на передачу со скоростью 400 Гбит/с предполагает внедрение нового типа оптических разъемов. Сильная сторона специализированных разработок этого направления (изделия SN компании Senko и MDC компании US Conec) – возможность эксплуатации в дуплексном и групповом вариантах, малые габариты и простота поддержки физической параллельной передачи. Изделия допускают одиночное и счетверенное применение. В последнем случае используется общая крепежная обойма, в которую обычные вилки вставляются под защелку. Процедуры коммутации при этом не меняются, так как обойма имеет механизм фиксации, идентичный механизмам отдельных вилок.

Справедливости ради отметим, что прямым предшественником SN и MDC может считаться изделие URM немецкой компании Euromicron, которое было разработано еще в начале 2000-х и нормировано стандартом IEC 61754-34. Непосредственное использование этого соединителя

для полноценной поддержки 400-гигабитных трактов затруднено из-за его неудовлетворительных габаритов: по площади миделя URM уступает своим более поздним аналогам примерно в 1,5 раза.

Обеспечение полярности дуплексных вилок

При организации дуплексных трактов по оптическим кабелям с ленточными волокнами необходимо обеспечивать правильную полярность. Делать это с помощью шнуров двух типов неудобно с эксплуатационной точки зрения. Поэтому ряд компаний предлагает универсальные конструкции, которые позволяют простыми средствами переключать полярность непосредственно на объекте. Разработки применимы как к моноблочным, так и к дуплексным вилкам, и базируются на различных принципах.

Например, существуют схемы на основе перестановки (рис. 1а) и поворота отдельных вилок (рис. 1б). В первом случае вилки переставляются в крепежных гнездах, во втором – поворачиваются вокруг своей оси с последующим переносом защитной крышки.

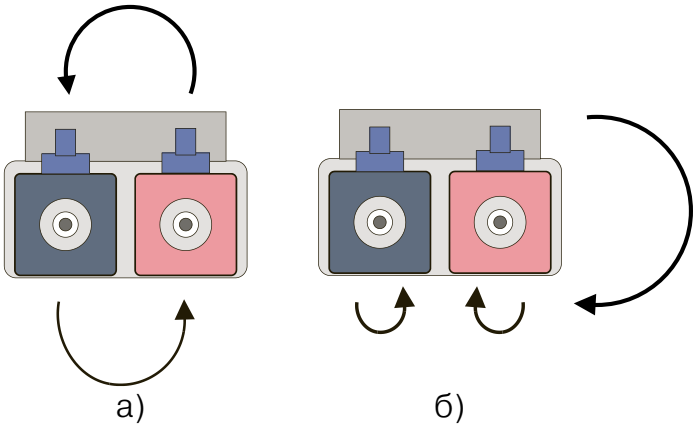
Снижение чувствительности к загрязнениям торцевой поверхности волокон

В процессе эксплуатации торцевые поверхности волоконного световода неизбежно загрязняются. Это происходит из-за того, что даже при соблюдении самых жестких норм на чистоту воздуха, принятых для технических помещений, в воздухе присутствуют взвешенные пылевидные частицы. Свой вклад может внести и нарушение правил эксплуатации элементов оптического соединителя.

Из-за малого диаметра световедущей сердцевины наиболее чувствительны к загрязнениям одномодовые соединители. До уровня практического применения доведены два способа решения этой проблемы.

Первый способ – расширение луча. На пути распространения оптического сигнала устанавливается микролинза той или иной формы, к которой непосредственно пристыковывается торец световода. За счет увеличения диаметра луча потери, возникающие из-за загрязнений, уменьшаются пропорционально увеличению площади (рис. 2).

Технология PRECONNECT Lotus, анонсированная в 2017 г. и продвигаемая немецкой компанией Rosenberger OSI (Optical Solutions and Infrastructures), предполагает нанесение на торцевую поверхность световода специального покрытия. Его структура предельно точно воспроизводит структуру верхней поверхности листьев лотоса, в результате чего частицы пыли просто соскальзывают с него (здесь используется так называемый эффект лотоса: лепестки и листья лотоса выделяют воскоподобное вещество, которое образует на поверхности особую структуру (нанорельеф) в виде микроскопических выступов, благодаря чему их поверхность отличается крайне низкой смачиваемостью. – *Прим. ред.*).

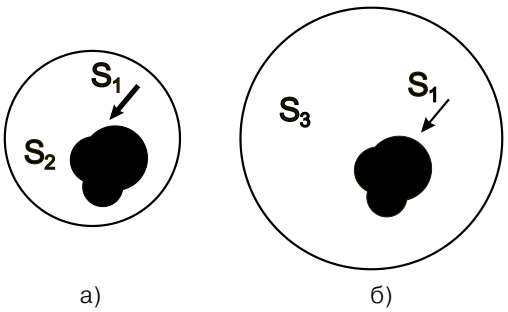


▲ **Рис. 1. Основные схемы изменения полярности дуплексных вилок разъема LC: а) перестановка вилок без переноса защитного козырька; б) поворот отдельных вилок дуплексной структуры на 180° с переносом защитного козырька**

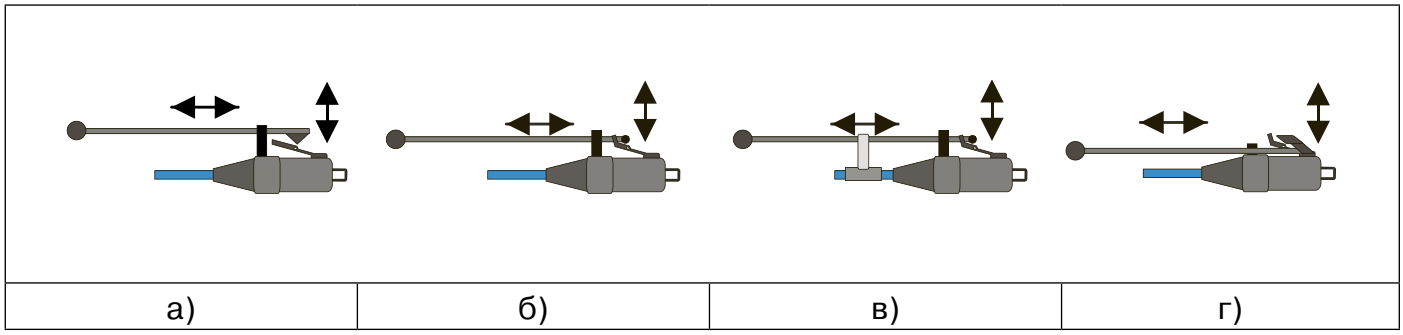
Схема push-pull

Коммутационное оборудование, используемое в оптической подсистеме структурированного каблирования ЦОДа, должно обязательно иметь высокую конструктивную плотность. Механизм фиксации вилки LC как стандартного дуплексного соединителя реализован на основе рычажной защелки, которая требует для отключения пустого пространства в районе свободного конца рычага под большой или указательный палец выполняющего эту операцию человека. Данное обстоятельство серьезно ограничивает плотность конструкции коммутационного устройства и не позволяет увеличить ее более определенного предела.

Для преодоления этого ограничения в конструкцию вилки LC без изменения формфактора той ее части, которая взаимодействует с гнездом розетки, внедряют различные варианты тяг и иных механических элементов. Их использование позволяет отключать вилку без не-



◀ **Рис. 2. Влияние загрязнений оптически активных поверхностей на затухание оптического разъема: а) обычная сердцевина; б) параллельный пучок света увеличенного диаметра**



▲ **Рис. 3. Варианты исполнения тяг механизма верхнего нажима дуплексных вилок LC для подключения к панелям высокой плотности: а) верхняя стержневая тяга, взаимодействующая с прямым рычагом; б) верхняя стержневая тяга, взаимодействующая с изогнутым рычагом; в) верхняя стержневая тяга с дополнительным подвижным креплением к кабелю; г) нижняя стержневая тяга с верхним прижимом**

посредственного доступа к свободному концу рычага.

Наиболее простой вариант заключается в адаптации к LC схемы push-pull, которая ранее применялась в его предшественниках: разъеме SC и миниатюрном MU. В этом случае нажатие на рычаг при отключении происходит за счет приложения тянущего осевого усилия к специально предназначенной для этого жесткой или мягкой тяге (рис. 3). Применение для этой цели защитного хвостовика встречается заметно реже.

Иногда разработчик отказывается от тяги в пользу рычажного механизма. Выигрыш в данном случае достигается за счет того, что точка приложения нажимающего усилия сдвигается назад, а передача отключающего воздействия на рычаг осуществляется с помощью системы рычагов. Малая популярность такого подхода объясняется кинематической сложностью схемы.

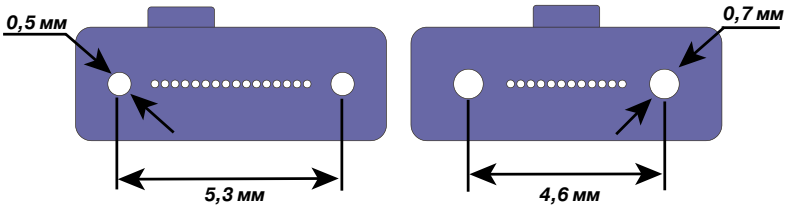
Учет перспектив внедрения 400-гигабитных линий в групповых конструкциях

Стандартные для ЦОДов групповые разъемы типа MPO/MTP, которые изначально были предназначены для организации физической параллельной передачи, потенциально могут армировать до 72 волокон в форме шести расположенных друг над другом групп по 12 волокон. 12-волоконный шаг отдельной группы невыгоден при организации параллельной передачи. Более удобные четырех- и восьмиволоконные схемы легко реализуются на типовых соединителях. 16-волоконная схема, необходимая для перспективных скоростей 400 Гбит/с, требует уже двухрядного расположения, что приводит к повышенным потерям.

Для того чтобы не прибегать к двухрядному расположению, в стандартный наконечник MT добавляют еще четыре посадочных места для получения соединителя MPO/MTP-16/32. Чтобы предотвратить ошибочное подключение к MPO/MTP-12, используется тройная механическая блокировка (рис. 4):

- боковое смещение направляющего выступа;
- изменение расстояния между центрирующими штифтами;
- уменьшение диаметра центрирующих штифтов.

Рис. 4. Схемы размещения световодов, выравнивающих штифтов и ключевых кодирующих выступов в однорядных 12- и 16-волоконных наконечниках соединителей MTP ▼



Внедрение групповых универсальных конструкций

Схема разъема MPO/MTP предполагает существование четырех различных вариантов вилки в зависимости от наличия или отсутствия центрирующих штифтов и расположения направляющего выступа на одной из широких граней наконечника, вследствие чего такая конструкция неудобна в эксплуатации. Наибольшим удобством среди серийных продуктов отличаются изделия компаний Panduit (PanMPO), Senko (MPO Plus) и US Conec (MTP PRO).

Конструктивная схема Panduit основана на разборном корпусе, который позволяет перемещать выполненную в форме салазок сборку направляющих штифтов в переднее и заднее положения с фиксацией под защелку и переносить направляющий выступ прямым поворотом обойменного фиксатора.

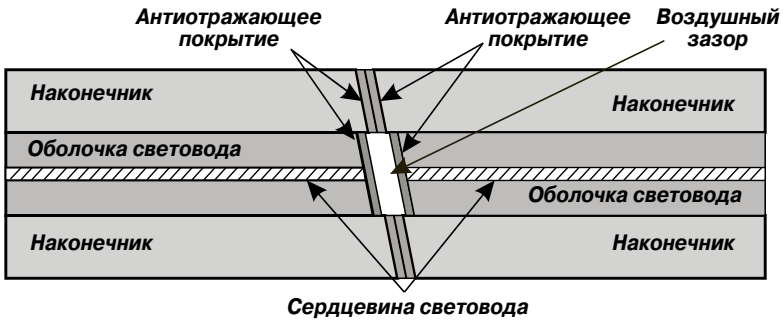
Изделия компаний US Conec и Senko выгодно отличаются от PanMPO своими меньшими габаритами, но в процессе изменения гендерности и полярности требуют применения довольно дорогого ручного технологического приспособления.

Уменьшение уровня обратных отражений групповых разъемов

Быстродействующие лазеры одномодовых оптических передатчиков очень чувствительны к обратным отражениям. Мешающие влияния этой разновидности опасны значительными искажениями формы импульсов, нарушающими нормальное функционирование решающего устройства приемника, и создаются всеми элементами оптического тракта. Наибольший вклад в правильно собранную и реализованную на стандартных компонентах линию вносят разъемные соединители.

Типовой способ подавления обратных отражений до безопасного уровня на основе угловой полировки может применяться для всех типов соединителей, но его возможности для групповых разъемов ограничены из-за сложностей обеспечения надежного физического контакта всех световодов линейки. Кроме того, из-за большого усилия, прикладываемого в момент соединения, исходная полировка быстро разрушается, что сопровождается ростом уровня отражений даже в угловых соединителях.

Для подавления обратных отражений можно воспользоваться антиотражающими покрытиями. Их установка также делает ненужным наличие прямого физического контакта торцов волокон или заменяющих их элементов в собранном разъеме, что существенно замедляет деградацию соединителя по обратным отражениям в процессе эксплуатации линии связи. Впервые такое решение было представлено в середине текущего десятилетия американской компанией Arrayed Fiberoptics, а схему реализующего ее соединителя демонстрирует рис. 5.



▲ **Рис. 5. Конструктивные особенности APC-наконечника MT компании Arrayed Fiberoptics и взаимодействие наконечников в собранном разъеме**

Отметим, что эффективность антиотражающего покрытия настолько велика, что компания Senko в своем разъеме Highdura MPO Plus даже отказалась от технически сложной угловой полировки.

■■■

Оптические соединители дуплексного и группового типа продолжают быстро развиваться. Основное направление их совершенствования – расширение функциональных возможностей и переход на универсальные конструкции, пригодные для применения в различных областях. ИКС

Специальные условия при оформлении подписки для корпоративных клиентов!

Оформляйте подписку
в редакции — по телефону: + 7 (495) 150-6424
или по e-mail: podpiska@iksmedia.ru

ИнформКурьер-Связь
ИКС
издается с 1992 года

Телеком • ИТ • Медиа
www.iksmedia.ru

Как создать топливохранилище для ЦОДа

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

Строительство топливохранилища – задача, казалось бы, давно решенная, но мы помним, сколько вопросов она вызвала, когда мы столкнулись с ней впервые. Поэтому считаем, что статья может быть полезна читателю, которому ранее не приходилось участвовать в создании такого рода объекта.

Практически каждому, кто имеет отношение к проектированию или строительству центров обработки данных, рано или поздно приходится укрупнять масштаб проекта, переходить от серверных и небольших ЦОДов к бóльшим по площади и энерговооруженности объектам. При этом он часто сталкивается с необходимостью увеличить время резервирования системы гарантированного питания и, как следствие, с необходимостью проектирования и строительства полноценного топливохранилища.

Для небольших ЦОДов многие традиционно обходятся либо встроенными в раму топливными расходными баками, либо баками, являющимися частью всепогодного контейнера. Но, как известно, емкость топливного бака, размещенного вместе с ДГУ, в общем случае законодательно ограничена 1 куб. м, что позволяет снабжать топливом дизельную установку мощностью 300–350 кВт в течение 12 ч (средний расход топлива составляет 0,16–0,19 л/(кВт•ч)). В случае повышения мощности объекта до нескольких мегаватт время резервирования системы гарантированного энергоснабжения от баков такой емкости уменьшается пропорционально.

В российской строительной практике топливохранилища разделяются по способу размещения резервуаров хранения на два основных типа: наземные и подземные. К подземным относятся топливохранилища с резервуарами, в которых уровень топлива не менее чем на 0,2 м ниже наименьшей отметки прилегающей к ним территории. Все остальные относятся к наземным. Наземные хранилища могут, в свою очередь, иметь два различных исполнения: открытый резервуар (группа резервуаров) для установки в здании и контейнерное исполнение для размещения на уличных площадках.

Рассмотрим каждый из видов топливохранилищ более подробно.

Подземные топливохранилища

У таких топливохранилищ объем отдельного резервуара может варьироваться в диапазоне 3–100 куб. м. Подача топлива к ДГУ осуществля-

Рис.1. Резервуары подземного топливохранилища ▶

◀▲ Рис.2. Наземное топливохранилище внутренней установки

▲ Рис.3. Насосная станция внутренней установки

ется с помощью погружных насосов, причем в этом случае не нужно создавать насосную станцию для заправки резервуаров из автоцистерн, поскольку заправка происходит самотеком. Кроме того, при подобной схеме размещения не требуется предусматривать емкости для аварийного слива топлива.

Подземные топливохранилища (рис. 1) удобны также тем, что позволяют экономить пространство в помещениях ЦОДа. Однако при этом необходимо понимать, что площадь, которую займут в здании ЦОДа или на прилегающей к нему территории контейнерные решения и подземные топливохранилища, будет приблизительно одинаковой, поскольку над подземными сооружениями запрещено располагать элементы инфраструктуры, в том числе внешние блоки инженерных систем и проезжие полосы транспортной сети. Поэтому при разработке концепции ЦОДа, определяя потребность в прилегающих территориях и выбирая их компоновку, нужно заранее зарезервировать площади для размещения топливохранилищ.

Подземные хранилища обладают рядом существенных недостатков, которые обусловлены уличным расположением резервуаров. В большей части климатических зон в России зимние температуры отрицательные, что вынуждает использовать топливо, строго соответствующее сезону, во избежание его загустевания. И это необходимо учитывать при проектировании, строительстве и эксплуатации данного объекта. Также обязательно нужно предусмотреть подогрев топлива в резервуарах и внешних трубопроводах.

Подземная организация топливохранилища затрудняет сведение между собой внешних сетей коммуникаций, таких как водопровод, сети теплоснабжения, электроснабжения, канализации и, соответственно, топливопроводов.

Еще одна проблема – сложность создания системы фильтрации и очистки топлива. Поскольку данную систему необходимо реализовать в условиях подземного размещения топливохранилищ, требуется строительство дополнительных подземных подогреваемых емкостей и кессонов, существенно удорожающих систему.

Кроме того, обустройство подземного хранилища закономерно сопряжено с большим объемом земляных работ, а последующая эксплуатация резервуарного оборудования – со значительными неудобствами.

Часть перечисленных недостатков присуща и контейнерным хранилищам уличного исполнения.

Наземные топливохранилища в здании

В подобных сооружениях объем одного резервуара ограничен 3–25 куб. м, что может усложнить создание системы топливохранилища в крупном ЦОДе. Для подпитки дизельных генераторов также используются поверхностные или погружные насосы, но при такой конструкции хранилищ необходимо устанавливать насосные станции для заправки резервуаров из автоцистерн и слива топлива. Кроме того, потребуются резервуары для аварийного слива, емкость которых должна быть не менее 30% объема всего топливохранилища, что может существенно удорожить систему.

Наземные топливохранилища внутреннего исполнения отличают простота организации системы фильтрации и очистки топлива, которую можно расположить в том же объеме обогреваемого помещения, что и сами резервуары. Это же обусловливает и удобство эксплуатации резервуарного оборудования, к которому имеется открытый доступ со всех сторон (рис. 2, 3).

Контейнерные топливохранилища наземной установки

Основное достоинство контейнеров заключается в том, что они являются изделиями полной заводской готовности, в них уже встроены насосы и вся необходимая арматура как для за-

Рис.4. Контейнерные топливохранилища ▶

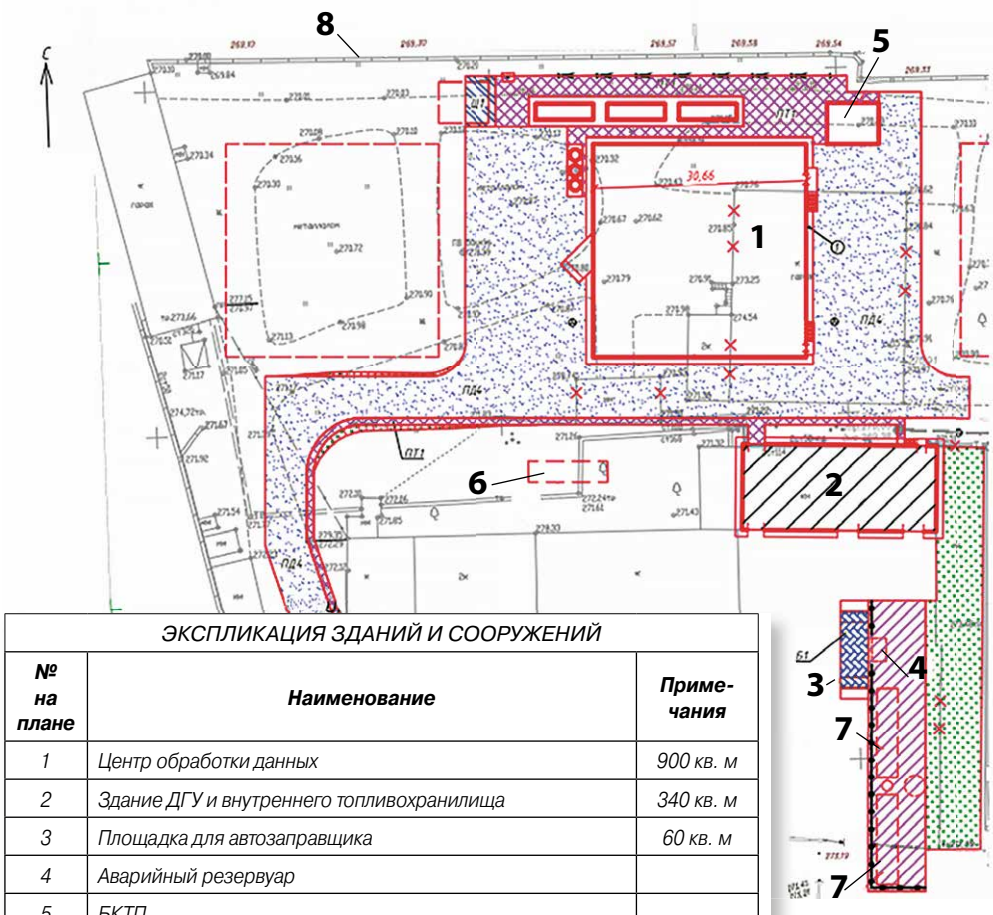
правки самого резервуара, так и для выдачи топлива (рис. 4). Зачастую данные изделия комплектуются встроенной системой автоматики, требующей лишь частичной донастройки под конкретный объект.

Недостатком же контейнеров являются более жесткие требования к их размещению на территории, прилегающей к ЦОДу, – согласно нормативным документам, все расстояния между элементами инфраструктуры контейнерного топливохранилища в два раза больше, чем у подземных. Кроме того, к недостаткам относятся перечисленные выше сложности, связанные с наружным размещением резервуаров.

Примеры организации размещения систем топливоснабжения

Рассмотрим создание топливохранилища емкостью 80 куб. м, которое способно в течение 12 ч обеспечивать топливом ЦОД расчетной мощностью 7,3 МВт. Площадь для него составит примерно 140 кв. м. Сюда входят как площади для размещения резервуарного парка и вспомогательного оборудования, так и прилегающая территория – площадка для автоцистерны, подъездные пути для ее проезда и маневрирования. Планировочное решение данного объекта, которое было реализовано на практике, приведено на рис. 5.

Рис.5. Генплан территории сооружений ЦОДа ▼



ЭКСПЛИКАЦИЯ ЗДАНИЙ И СООРУЖЕНИЙ

№ на плане	Наименование	Примечания
1	Центр обработки данных	900 кв. м
2	Здание ДГУ и внутреннего топливохранилища	340 кв. м
3	Площадка для автозаправщика	60 кв. м
4	Аварийный резервуар	
5	БКТП	
6	Резервуар для сбора поверхностных стоков, V = 80 куб. м	
7	Пожарный резервуар, V = 85 куб. м	
8	Ограждение бетонное, H = 1,8 м	

На другом объекте было построено топливохранилище подземного типа, рассчитанное на 15 куб. м топлива и способное обеспечивать работу ЦОДа мощностью 1,9 МВт в течение 24 ч. Оно располагалось внутри здания и площадь для него составила порядка 80 кв. м.

Дополнительное проектирование и пожарная безопасность

При проектировании системы топливоснабжения нельзя забывать о сопутствующих объектах, проектировочные решения для которых должны быть включены в смежные разделы документации. Так, в разде-

ле, посвященном железобетонным конструкциям, должны быть предусмотрены основы для крепления топливных резервуаров, а в случае необходимости – системы лотков для прокладки топливопроводов. Могут потребоваться металлические конструкции для размещения вспомогательных расходных баков внутри помещения. Следует помнить и об электроснабжении оборудования топливохранилища, а именно насосного оборудования, системы автоматики и системы подогрева резервуаров и топливопроводов.

В проектную документацию системы топливоснабжения необходимо также включить раздел, посвященный автоматизации системы топливоснабжения, управлению насосным оборудованием, системой фильтрации и рециркуляции. В этом разделе должны быть определены мероприятия по защите хранимого топлива от расслоения, загрязнения и загустевания. Кроме того, требуется реализовать систему защиты от перелива и предупреждения об уровне топлива в резервных емкостях.

Плотность компоновки оборудования на площадке ЦОДа зачастую делает невозможным соблюдение всех требуемых нормами противопожарной безопасности расстояний между зданиями и сооружениями и заставляет от этих норм и правил отступать с обязательным обоснованием таких отступлений. Обоснование сводится либо к выпуску специальных технических условий (СТУ) по пожарной безопасности, описывающих вынужденные отступления и компенсирующие их мероприятия, либо к выполнению расчета пожарного риска.

Кроме того, топливохранилище должно в обязательном порядке пройти регистрацию как опасный производственный объект. Согласно Федеральному закону «О промышленной безопасности опасных производственных объектов» от 21.07.1997 № 116-ФЗ, топливохранилище в составе ЦОДа является опасным производственным объектом, на котором горючие жидкости используются в технологическом процессе. Данные объекты подлежат регистрации в государственном реестре в порядке, установленном Правительством РФ.

Поэтому, чтобы избежать серьезных проблем с размещением топливохранилища или выпуском сложных СТУ, мы настоятельно рекомендуем на самых ранних этапах проектирования либо выработки концепции ЦОДа привлекать к созданию планировочных решений прилегающих территорий компании, специализирующиеся на подобных объектах инфраструктуры. ИКС

RUSSIAN DATA CENTER AWARDS DC 2020

IV профессиональная Премия в области создания и услуг дата-центров

Торжественная церемония награждения состоится 22 сентября 2020 года

Церемония награждения лучших реализованных проектов в области ЦОДов в России и странах СНГ. Жюри Премии состоит из известных российских и зарубежных экспертов, которые обладают многолетним опытом реализации проектов дата-центров. Выбор победителей Премии происходит путем голосования членов жюри по представленным документам и описаниям проектов.

Получить информацию о номинациях и подать заявку на участие в конкурсе можно на сайте dcawards.ru

Реклама 16+

В поисках мультиклауда

Николай Носов

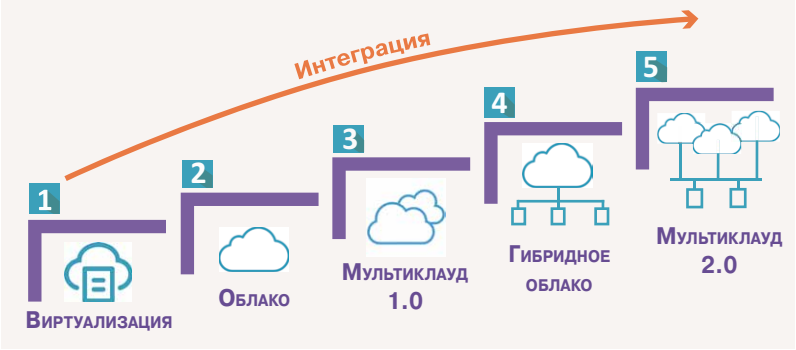
Облачные услуги постепенно стали необходимы бизнесу как воздух – или, вернее, как электричество. По-настоящему удобны они делаются тогда, когда их можно использовать по мультиклаудной модели: брать разные услуги у разных провайдеров и легко их менять.

Появление облачных технологий любили сравнивать с появлением электричества. Когда-то в жилище с наступлением темноты зажигали свечи или керосиновую лампу. Теперь достаточно щелкнуть выключателем. И не надо думать, какая ГЭС произвела электричество, какая электросеть его доставила. Магистральные сети страны связаны, нехватка мощности в одном районе легко компенсируется свободными мощностями другого.

В облачных технологиях до этого еще не дошло, и потребитель должен сам выбирать, какую «ГЭС» использовать, разбираться в ее особенностях и подстраивать под нее свое оборудование. Но процесс идет. Облачные услуги все больше становятся типовыми, успех нового сервиса у одного облачного провайдера приводит к появлению аналогичных сервисов у конкурентов. Потребитель не хочет быть привязан к одной «электростанции», ему нужна свобода выбора. У одного поставщика выгоднее тариф на одну услугу, у другого – на другую. Один провайдер предлагает отличное решение в области финансов, другой – в лингвистике. Хочется взять все лучшее, чтобы все работало в комплексе, но без жесткой привязки к поставщикам услуг, чтобы при изменении ситуации можно было безболезненно перенести сервис от одного провайдера к другому. Перейти к связанности «магистральных сетей», к использованию мультиоблака.

От облака к мультиклауду

Термин «мультиклауд» и его перевод «мультиоблако» употребляются в статьях и докладах на конференциях все чаще. При этом специалисты понимают термин по-разному. Попробуем разобраться, какой смысл вкладывают в него эксперты на российском рынке.



▲ Рис. 1. Этапы развития мультиоблачных технологий

В самом использовании нескольких облаков нет ничего нового. Еще лет восемь назад в банке, где я работал, по модели SaaS функционировала система интернет-банкинга, расположенная в облаке ЦФТ в Новосибирске, у другого провайдера размещалась почта, у третьего – веб-сайт организации. Формально можно считать, что уже тогда у нас было мультиоблако, хотя такого термина мы не знали. В терминологии архитектора облачных решений компании Crayon Андрея Дубровина у нас был «мультиклауд 1.0» – традиционное решение, подразумевающее использование нескольких облачных сервисов от разных провайдеров.

Сейчас у большинства специалистов сформировалось понимание, что мультиклауд – это нечто большее – некая интегрированная система из нескольких облаков (рис. 1). Если смотреть с точки зрения облачного провайдера, то она должна быть как минимум объединена общим биллингом. Например, по такой схеме работает ряд российских облачных провайдеров, предоставляющих доступ к облакам гиперскейлеров Amazon Web Services, Microsoft Azure, Google Cloud Platform и Alibaba Cloud и позиционирующих услугу как мультиоблачную. В этом случае клиент работает с одним поставщиком, что удобно прежде всего его

Илья Хала, генеральный директор, 3data

В моем понимании мультиклаудные вычисления – это потребление облачных сервисов от разных поставщиков или на разных платформах при построении единой интегрированной инфраструктуры заказчика. Например, когда клиент разворачивает инфраструктуру в облаках двух разных провайдеров, которые резервируют друг друга для обеспечения отказоустойчивости, или инфраструктура распределяется между облаками на разных платформах для использования преимуществ каждой них при решении конкретных задач. То есть мультиклауд предполагает администрирование нескольких облаков. Специальные программные инструменты для единообразного управления разными облаками помогают повысить эффективность мультиклаудных инфраструктур. А вот системы, распределенные по разным кластерам (зонам доступности) одной платформы одного провайдера, скажем, традиционные решения для обеспечения катастрофоустойчивости, я мультиклаудом не считаю. Хотя, возможно, в будущем понятие мультиклауда будет расширено и на такие случаи.

Андрей Гусев, руководитель направления по решениям для управления облачной инфраструктурой, IBM в России и СНГ

Мультиоблако – это не обязательно несколько разных облачных провайдеров и/или платформ разных вендоров.

бухгалтерии: можно получить сводную ведомость по расчетам с разными облаками и все необходимые финансовые документы, да еще и произвести оплату в рублях.

А вот, скажем, Gartner не акцентирует внимание на биллинге, считая, что мультиоблако – это несколько сервисов облачных вычислений в единой гетерогенной архитектуре, используемой для ослабления зависимости от отдельных поставщиков, повышения гибкости и предотвращения аварийных ситуаций. От гибридного облака оно отличается тем, что охватывает несколько провайдеров общедоступных облаков, а не несколько режимов развертывания (публичный, частный).

Шире трактует понятие IDC, включая в мультиклауд помимо публичных частные облака: «Мультиклауд – это организационная стратегия или архитектурный подход к проектированию сложной цифровой услуги, которая включает использование облачных услуг более чем одного поставщика сервисов. Это могут быть частные облачные сервисы, сервисы вычислений в публичном облаке, хранилища общедоступных объектов от нескольких провайдеров или IaaS- и SaaS-сервисы от одного или нескольких провайдеров облачных сервисов».

Компания VMware включает в свое определение мультиклауда и гибридное облако. Так, архитектор бизнес-решений VMware в России и СНГ Артем Гениев считает, что оно является подвидом мультиоблака в случае, когда помимо собственных on-premise-облаков компания использует облака нескольких провайдеров.

А некоторые эксперты считают целесообразным выделять два вида мультиклауда – частный и гибридный. Частный мультиклауд объединяет несколько частных облаков – например, облака на Hyper-V, VMware и OpenStack. Основная задача такой системы – интеграция управления и мониторинга частных облаков. Гибридный мультиклауд – это публичные облака нескольких провайдеров плюс частная инфраструктура. «Многие банки используют облако для размещения сред разработки и тестирования, но при этом оставляют в частной инфраструктуре продуктив, который нужно контролировать строже. В этом случае публичные облака увеличивают мощность частной инфраструктуры, что особенно актуально в отраслях, которые только прошли или проходят цифровизацию. Кроме того, привлечение публичных аутсорсеров-разработчиков тоже стимулирует «гибрид»: пустить их в публичное облако безопаснее, чем в частную корпоративную систему», – поясняет руководитель Mail.ru Cloud Solutions Илья Летунов.

Рис. 2.
Наиболее важные характеристики мультиклауда ▼

Источник: iksmedia.ru

Функциональный подход

К определению понятия «мультиклауд» можно подходить через его характеристики. Судя по итогам голосования на сайте iksmedia.ru, наиболее важной характеристикой для мультиклауда (35% ответов) является наличие единой системы управления несколькими облаками (рис. 2). Отмечались также «возможность автоматизированной переброски нагрузки между облаками» (17% проголосовавших выделили эту характеристику как наиболее важную), «использование конкурирующих сервисов из нескольких облаков» (11%).

В опросе, который был проведен в группе RCCPA на Facebook, предлагалось указать несколько характеристик, обязательных для того, чтобы решение относилось к мультиоблачным. Помимо очевидной характеристики – наличия нескольких облаков, эксперты выделили возможность автоматизированной переброски нагрузки между облаками. То есть мнение, что мультиоблако – это не только набор используемых облаков («мультиклауд 1.0»), но и многооблачный сервис с возможностью миграции между облаками, на нашем рынке уже сложилось.

Важность переброски нагрузки между облаками отметили и опрошенные «ИКС» эксперты. «Мультиклауд – это в первую очередь возможность быстрой и прозрачной для пользователей миграции рабочих нагрузок между различными поставщиками облачных услуг», – заявил руководитель департамента R&D ActiveCloud Сергей Горлинский.

Интересный результат – невысокий процент опрошенных экспертов RCCPA, считающих необходимым свойством мультиклауда наличие единой системы биллинга. Так, заместитель генерального директора Selectel Сергей Пимков уверен: «Единый биллинг, панель управления, способ оплаты или автоматизация развертывания не яв-

ляются неотъемлемыми элементами мультиклаудного решения. Эти возможности лишь повышают удобство его использования, а в ряде случаев выступают потенциальным источником проблем. Например, общий биллинг в такой системе может стать единой точкой отказа». Но у отнесения единого биллинга к необходимым свойствам мультиоблака есть и сторонники.

В то же время многие эксперты рассматривают как критически важную для мультиклауда единую систему управления несколькими облаками. По мнению И. Летунова, основное преимущество мультиоблачной архитектуры – это интеграция: общая панель управления сервисами разных поставщиков с агрегированными управлением, мониторингом, биллингом и отчетом по расходам. В части управления важно, что мультиклауд позволяет обслуживать облака самостоятельно, без ручных операций со стороны провайдеров.

Схожее мнение о необходимости единой системы управления имеет и директор NetApp в России и СНГ Татьяна Бочарникова: «Наиболее важными свойствами на сегодня считаю возможность выбора сервисов из нескольких облаков, наличие единой системы управления ресурсами нескольких провайдеров и возможность беспроблемной переброски нагрузки между облаками».

И конечно, важная функция мультиклауда – обеспечение отказоустойчивости. В этом случае использование разных облачных провайдеров является обязательным, поскольку ликвидирует единую точку отказа.

В целом же определение мультиклауда (мультиоблака) еще не устоялось. «Мультиклауд – очередной маркетинговый термин в сфере облачных услуг, – уверен директор практики облачных решений AT Consulting Михаил Бараблин. – Значение во многом зависит от желаний продавцов, в каждом отдельном случае оно свое. Тем не менее общий смысл есть».

Оптимистично настроен Дмитрий Хороших, менеджер по развитию бизнеса Cisco: «Ситуация очень похожа на ту, что была 10 лет назад с «просто облаками». Сегодня Cisco рассматривает мультиклауд как систему, которая позволяет один раз задать структуру приложения, определить состав его компонентов, связей между ними, требований к вычислительным ресурсам, сетевой связности и безопасности. А затем единообразно размещать это приложение в частном или публичном облаке, возможно, даже разнести компоненты по разным облакам. При этом все установленные требования должны выполняться и должны осуществляться мониторинг приложения в целом и единое управление его стоимостью. Звучит как фантастика, но на современном уровне развития технологий здесь нет ничего невозможного».

Мультиклауд: сценарии и задачи

Бизнес-цель мультиклауда – оптимизация процессов за счет использования разных облаков. А распределение нагрузок между облачными провайдерами повышает отказоустойчивость решений.

Обычно переход к использованию нескольких облаков происходит стихийно и неосознанно: в подразделениях организации подключаются к различным нужным для бизнеса сервисам, которые предоставляются в разных облаках (см. рисунок). Иногда с облаками начинают работать, не ставя в известность ИТ-службы предприятия, и впоследствии приходится прилагать массу усилий, чтобы обеспечить безопасность «теневых ИТ» – несогласованных, но уже задействованных в бизнес-процессах сервисов, – и интегрировать их в существующую систему. Новые облака могут появляться в результате поглощения других компаний с их бизнес-

ПОЧЕМУ КОМПАНИИ НАЧИНАЮТ ИСПОЛЬЗОВАТЬ МУЛЬТИКЛАУД

Сергей Горлинский, руководитель департамента R&D, ActiveCloud

Облачные провайдеры сегодня предлагают разнообразные сервисы. И зачастую, чтобы получить оптимальное с технологической и финансовой точки зрения решение, требуется задействовать несколько провайдеров. Один провайдер может дать интересное решение для хранения данных, другой предоставляет интеллектуальную систему отражения атак, третий – услугу «база данных как сервис». Использование мультиклауда позволяет заказчику не стать заложником одного поставщика услуг.

процессами и ИТ-инфраструктурой, включая облачную составляющую.

Переход происходит и эволюционно. Так, в 90-х в банке, где я работал, по соображениям безопасности был полностью запрещен интернет. Необходимость пользования электронной почтой и создания веб-сайта привела к возникновению в банке сети с выходом в интернет, физически изолированной от основной сети банка. Долго такое решение не просуществовало – появился интернет-банкинг, для которого нужен оперативный обмен данными с автоматизированной банковской системой, Центробанк начал запрашивать отчетные формы через интернет. По VPN-каналам через Глобальную сеть стали подключаться дополнительные офисы, кассы, банкоматы. Требовался безопасный доступ к внутренней сети, который удалось реализовать с помощью межсетевых экранов и демилитаризованных зон.

Юрий Новиков, руководитель направления развития облачных технологий, Softline

Важно отметить, что, используя сервисы одного поставщика облаков, экономическую эффективность можно повысить лишь до определенного уровня. Есть сервисы дешевые и медленные, есть дорогие и быстрые, и заказчик вынужден потреблять и те и другие у одного провайдера. Однако, перейдя в мультиклаудную инфраструктуру, можно повысить качество и снизить стоимость этих сервисов: у разных провайдеров можно потреблять разные сервисы, именно те, в которых они сильны.

В итоге сети объединились, и банк пришел к простой слабосвязанной мультиоблачной системе, которая описывается термином «мультиклауд 1.0». Дальнейшую эволюцию прервал отзыв лицензии. Но работы по переносу бизнес-процессов в облако уже шли. В облако ЦФТ отдали систему интернет-банкинга, что сильно разгрузило службу ИТ. Рассматривался вариант полного переноса банковских систем в облако ЦФТ, что уже сделали некоторые банки. Не выглядел фантастикой и дальнейший путь развития – не выступать точкой интеграции облачных сервисов, а передать ее облачному провайдеру, оставив за собой контроль и мониторинг процессов.

Отдать ИТ на аутсорсинг

Сценарий аутсорсинга ИТ высвобождает ресурсы компании для решения основных бизнес-задач, но еще больше привязывает к поставщику услуг, который может воспользоваться выгодным положением и замкнуть на себя максимально возможное количество сервисов. Передача точки интеграции облаков провайдеру только усилит зависимость, что негативно сказывается на бизнесе, которому нужна гибкость, возможность выбора между конкурирующими поставщиками решений.

Поэтому полный перенос, скажем, банковских систем в облако стороннего провайдера – редко встречающийся сценарий на российском рынке. Банки предпочитают эксплуатировать АБС на своих площадках, где они могут сами заниматься защитой чувствительных для бизнеса данных, сохранять тайну вкладов и контролировать состояние счетов.

При этом облака задействуются как резерв вычислительной мощности, например, при тестировании. Так, в Райффайзенбанке облако AWS служит для расширения внутренних ресурсов в случае пиковых нагрузок при многопоточном выполнении автоматизированных UI-тестов – проверке качества продукта при каждом внесении изменений разработчиками. Если расширить подход и масштабировать тесты в нескольких облаках, выбирая наиболее выгодные на данный момент тарифы, то получим сценарий применения мультиоблака.

Выбрать лучший функционал

Предположим, мы хотим для минимизации репутационных рисков оперативно находить негативные отзывы о компании в Facebook. Отзывов бывает много, причем на разных языках. Облака предлагают разные по возможностям сервисы перевода. Для того чтобы использовать лучшие, придется заниматься интеграцией облаков. Например, в SaaS-решении компании YouScan, ко-

торое изначально базируется на Microsoft Azure, «под капотом» задействуются речевые технологии и «Яндекса», и Google, и AWS.

Для качественного сканирования и распознавания контента пользоваться сервисами только одного провайдера неэффективно. Так, с распознаванием английского языка лучше справится Microsoft, а если нужно распознать киргизский язык, то больше подойдет Yandex SpeechKit.

Выполнить требования регуляторов

Законодательные ограничения по защите данных существуют не только в России – аналогичные законы приняты и в других странах. Необходимость выполнения требований регуляторов заставляет международные компании искать локальных облачных провайдеров для размещения данных своих клиентов. Например, этим на российском рынке сейчас занимается международная компания по производству косметики Mary Kay.

Так же поступает один из клиентов «Яндекс.Облака», разработчик продуктов в сфере биоинформатики. По словам Олега Коверзнева, директора по развитию бизнеса «Яндекс.Облака», компания имеет единую архитектуру для работы во всех странах, при этом в каждом регионе выбирает местного облачного провайдера.

В итоге компания обзаводится несколькими облаками и переходит к мультиоблачной архитектуре.

Приблизиться к клиенту

Использование мощностей региональных облачных провайдеров помогает улучшить взаимодействие с конечными пользователями, обеспечить высокую доступность конечного сервиса. Так, во многих компьютерных играх, например, в популярной во всем мире белорусской игре World of Tanks, геймерам важна высокая скорость отклика, а эту задачу могут решить только региональные провайдеры, облачные площадки которых максимально приближены к пользователям.

Систему с edge-облаками для первичной обработки данных и центральным облаком для анализа предварительно обработанной информации в трактовке ряда экспертов также можно рассматривать как мультиоблако, несмотря на специфичность архитектуры. Во всяком случае под некоторые определения мультиклауда такие решения подходят.

Обеспечить отказоустойчивость

Перспективным выглядит использование мультиклауда для повышения устойчивости ИТ-систем к различным аварийным ситуациям – произошел ли в ЦОДе облачного провайдера пожар, перерубил ли экскаваторщик магистральный кабель, работоспособность бизнес-приложений пострадать не должна.

> Самый простой сценарий мультиклауда – это «теплый» резерв с полноценным переключением ИТ-системы на другую площадку с сохранением производительности.

Максим Захаренко, генеральный директор, «Облакотека»

На рынке уже предлагаются многоплатформенные системы резервного хранения данных и репликации виртуальных машин, решения для быстрого переключения ИТ-систем на другие площадки. В дальнейшем предполагается не ограничиваться простым резервированием критичных для бизнеса систем в другое облако, а создавать cloud native мультиоблачные отказоустойчивые системы.

«Индустрия стремится к созданию мультиклауда 2.0, который должен обеспечить абсолютную отказоустойчивость. В таком решении на базе микросервисной архитектуры каждая функция реализована как отдельный контейнер, а контейнеры распределены между несколькими облачными провайдерами», – поясняет архитектор облачных решений компании Crayon Андрей Дубровин.

Пока такое решение технически невозможно из-за сложностей сетевого взаимодействия между облаками и сервисами разных провайдеров. Например, контейнеры, работающие в облаке Microsoft Azure, не будут «доверять» контейнерам облака Amazon, поскольку у каждого провайдера есть своя служба цифровых сертификатов, и эти службы между собой не взаимодействуют. Для устранения проблемы можно привлечь дополнительного участника и использовать его решение. Но этот третий участник может стать точкой отказа. Остается ждать договоренностей между лидерами облачной отрасли.

Применение мультиоблачных решений требует серьезного аудита и изменений в устоявшихся процессах и технологиях. Зачастую нужны существенные изменения в архитектуре рабочих нагрузок, а иногда их полная переработка.

«К сожалению, нельзя просто взять и перевести рабочую нагрузку или приложение на рельсы мультиклауда – это комплексный, достаточно сложный и продолжительный по времени проект», – напоминает руководитель департамента R&D ActiveCloud Сергей Горлинский.

Мультиклауд: проблемы и перспективы

С увеличением количества используемых облаков возрастает сложность задач интеграции, контроля и обеспечения безопасности. Тем не менее постепенно мультиоблачный подход станет доминирующим.

Управление и учет

Несмотря на все преимущества мультиоблака, его использование сопряжено с целым рядом сложностей, которые важно учитывать (см. рисунок).

Даже при работе с одним облаком вести учет потребляемых ресурсов непросто, особенно на крупных предприятиях. Легко развернуть новые экземпляры виртуальных машин (инстансы), труднее понять, какие сервисы уже не нужны, и проконтролировать их отключение. Да и посчитать затраты на тысячи развернутых инстансов непросто, а с переходом к мультиоблакам задача усложняется еще больше.

СЛОЖНОСТИ ИСПОЛЬЗОВАНИЯ МУЛЬТИКЛАУДА

Бесконтрольное использование облаков сильно сказывается на бюджете, и бизнес ограничивает его за счет бюрократических процедур. Но долгие согласования с контролирующими подразделениями и службами информационной безопасности сводят на нет одно из основных преимуществ облачных решений – быстроту предоставления инфраструктуры.

Поэтому нужны автоматизированные системы для управления ресурсами в мультиоблаке. Попытки создания таких систем уже предпринимаются. Например, в мультиклаудном решении Cloud IQ компании Crayon единый биллинг и единая система управления позволяют заказчикам, работающим с несколькими видами облаков, получать всю информацию о подписках, их продлевать и расширять. Через единый интерфейс можно смотреть статистику, получать рекомендации о переносе тех или иных нагрузок между облаками, контролировать расход средств. Правда, пока такая система формируется для каждого конкретного заказчика и объединяет, к примеру, облака AWS и «Яндекса».

Технические сложности

Приложения для мультиоблачных сред предъявляют повышенные требования к разработчикам. «Чтобы заниматься дизайном или редизайном приложений для работы в мультиоблачной среде, архитекторы и специалисты по DevOps должны владеть современным ин-

Сергей Пимков, заместитель генерального директора, Selectel

Пользоваться мультиоблаком удобно, если есть единый биллинг и общая панель управления. Это самые очевидные ценности, которые агрегатор может предложить клиентам. Но создание единой панели и биллинга потребует существенных инвестиций. Вернуть их получится либо за счет повышения цен, либо благодаря большим объемам оказываемых услуг. Однако заметная разница между расценками агрегатора и провайдеров, скорее всего, отпугнет часть потенциальных клиентов. А пока услуга остается нишевой, не приходится рассчитывать и на быстрое масштабирование бизнеса. Но даже если агрегатор сможет предложить единый биллинг и управление и сохранить конкурентные цены, это не гарантирует ему успеха. Потому что в такой системе есть единая точка отказа, и в случае проблем на стороне агрегатора клиенты не смогут управлять всеми частями своего мультиоблака. Подобные риски неприемлемы, например, при реализации катастрофоустойчивых сценариев.

струментарием разработки, тестирования и развертывания приложений, иметь новые архитектурные навыки, например, построения микросервисных архитектур», – предупреждает руководитель группы архитекторов по решениям Red Hat Владимир Карагиоз.

Провайдеры публичных платформ ограничивают возможность построения доверительных отношений между платформами и зачастую не позволяют осуществить прозрачную интеграцию, например, с сохранением сетевой адресации. Технически сложной задачей является и прозрачная миграция виртуальных машин между различными системами виртуализации.

У облачных провайдеров не хватает открытых API для управления их сервисами. На отечественном рынке такие API есть, но их мало. «Задача заключается в том, чтобы с этими сервисами состыковаться. Фактически каждому клиенту необходимо разработать свою интеграционную систему, но это и дорого, и сложно. ИТ-службы клиентов не будут самостоятельно изготавливать софт, а рынка подобных интегрирующих систем в РФ точно нет», – подчеркивает генеральный директор «Облакотеки» Максим Захаренко.

Микросервисная архитектура рассматривается экспертами как фундамент мультиклауда, контейнеры – как основной инструмент управления. Следующий шаг – создание прямых CDN-сетей между облачными провайдерами.

Сейчас эта задача решается через сторонние компании – телеком-операторов. Например, «Ростелеком» может создать отдельный выделенный канал между облаками «Яндекса» и Mail.ru, но в идеале, как отмечает архитектор облачных решений компании Crayon Андрей Дубровин, нужно, чтобы между этими двумя провайдерами был их собственный канал. Это поможет избежать дополнительной финансовой нагрузки, которая в случае участия телеком-оператора ложится на плечи конечного потребителя. Кроме того, посредник снижает уровень безопасности мультиклауда, поскольку становится единой точкой отказа.

С увеличением числа облаков возрастают сложности в реализации политик безопасности, принятых в организации. Один из вариантов решения проблемы – создание отдельного слоя, транслирующего политики предприятия в подключаемые облака. Примером может служить Cisco Cloud ACI – комплексное решение для автоматического подключения к сети, согласованного управления политиками и упрощенных операций для сред с несколькими облаками.

Перенос данных

Узким местом при использовании мультиоблака является перенос между разными облаками больших объемов данных. Выходом из положения здесь может стать хранение массивов информации в отдельном частном или публичном облаке с возможностью переброски вычислительной нагрузки между сторонними облаками.

Например, с помощью технологий NetApp Data Fabric немецкий сервис-провайдер DARZ предлагает клиентам возможность практически мгновенного переноса рабочих нагрузок между облаками разных гиперскейлеров, в том числе AWS, Microsoft Azure, IBM Bluemix/Softlayer.

Используя свое конкурентное преимущество – доминирование на рынке СУБД, корпорация Oracle смогла заключить партнерское соглашение с компанией Microsoft, направленное на обеспечение совместимости облачных сред. В результате заказчики получат возможность перемещать критически важные рабочие нагрузки между Microsoft Azure и Oracle Cloud. Предприятия смогут беспрепятственно подключать облачные сервисы Azure, такие как Analytics и AI, к облачным сервисам Oracle Cloud, включая автономную базу данных Autonomous Database, и выполнять одну часть рабочей нагрузки в Azure, а другую часть той же рабочей нагрузки – в облаке Oracle Cloud. Таким образом, клиенту, хранящему данные в БД Oracle on-premise или в Oracle Cloud, при использовании сервисов Microsoft Azure не придется перебрасывать данные в облако Microsoft.

Провайдеры против клиентов

Клиенты заинтересованы в легкой смене используемых облачных сервисов. Но это противоречит интересам провайдеров, которые хотят привязать клиента к себе. Когда у одного из ли-

> Контейнеры, в том числе под управлением Kubernetes, позволят сделать мультиклауд единым, поскольку поддерживают единый формат, де-факто стандартный для всех современных микросервисных приложений. Существуют решения, которые упрощают развертывание микросервисных приложений в мультиклауде. Однако проблема совместимости виртуальных машин на базе Hyper-V, VMware, KVM останется актуальной. Так что ключом к развитию мультиклауда будет возможность мигрировать из одного облака в другое, мобильность клиента без привязки к вендору.

Илья Летунов, руководитель платформы, Mail.ru Cloud Solutions

Артем Гениев, архитектор бизнес-решений, VMware в России и СНГ

Для того чтобы в России появился устойчивый локальный рынок решений для мультиоблака, либо должно заметно усилиться присутствие гиперскейлеров (AWS, Azure, Google Cloud) в сегментах средних и крупных предприятий, либо возникнуть устойчивые и сравнимые по зрелости и функциональному охвату экосистемы сугубо российских провайдеров.

деров рынка появляется новый сервис, другие стараются повторить услугу в своем облаке, чтобы у клиентов не возникало соблазна перейти к конкуренту. У поставщиков облачных услуг не видно стимулов к созданию среды, в которой клиенту будет легко уйти от их сервисов и сформировать собственное мультиоблако.

Зато облачному провайдеру есть смысл вступить в альянс с партнером, расширяющим клиентскую базу за счет предложения новых услуг. Примером служат партнерские отношения между лидерами рынка публичных облаков и по-прежнему занимающей ведущие позиции на рынке частных облаков VMware. Компания не рассматривается как конкурент – своих публичных облаков у VMware нет. Зато уже существуют гибридные облака VMware с Oracle, Azure, Google Cloud и AWS.

Олег Коверзнев, директор по развитию бизнеса, «Яндекс.Облако»

Мы хорошо понимаем, что мультиклаудная модель – наиболее перспективный путь применения облачных сервисов в бизнесе.

В качестве третьей стороны, объединяющей облака, пытается выступать Veeam Software, перебрасывающая образы виртуальных машин на платформы гиперскейлеров AWS, Microsoft Azure и IBM Cloud. В качестве объединяющего узла можно рассматривать и клауд-брокеров – посредников между несколькими провайдерами и заказчиком, которые берут на себя функцию поиска и предоставления наиболее выгодного облачного сервиса.

А вот сами гиперскейлеры идут на объединение неохотно, разве что под давлением очень крупного заказчика. Возможно, что победа Microsoft в облачном тендере Пентагона на $10 млрд неслучайно совпала с заключением партнерства с Oracle. Практика покажет, как гиганты смогут согласовать свои стандарты и прямо конкурирующие сервисы, например, Azure Machine Learning и In-Database Machine Learning от Oracle.

«Общие проблемы – отсутствие стандартов в процессах и технологиях оказания облачных услуг. Например, нет типовых API для заказа услуг у провайдеров. Провайдерам это не нужно. Возможно, появление государственного облачного брокера начнет менять рынок, но я смотрю на это скептически», – говорит директор практики облачных решений AT Consulting Михаил Бараблин.

Перспективы в России

Простейший мультиклауд (мультиклауд 1.0) с несколькими не связанными между собой облаками широко используется в России. Хостинг веб-сайта в одном облаке, бизнес-приложение в другом, отправка отчетности в третьем... Но мультиклауд в современном понимании, с глубокой интеграцией облаков – дело будущего. «Мультиклаудная модель массовой в ближайшее время не станет, основная часть российских компаний делает только первые шаги в освоении облаков», – считает и директор по развитию бизнеса «Яндекс.Облако» Олег Коверзнев.

Количество российских компаний, задействующих мультикладную модель, будет расти в сегментах наиболее активных пользователей облачных платформ – в ИТ, ритейле и финансовом секторе. Скажется и давление регуляторов, заставляющих все большее количество сервисов и данных переносить на территорию России и тем самым использовать и западные, и отечественные облака, а также облака с повышенными требованиями к безопасности. При этом перенос сервисов в российские облака ограничит применение передовых мультиклаудных технологий зарубежных гиперскейлеров, в которых отечественные провайдеры пока отстают.

Взгляд в будущее

Продолжая сравнение облачных вычислений с электричеством, отметим, что полной стандартизации энергоснабжения не произошло. В одних странах напряжение 127 В, в других – 220 В. Туристам приходится искать переходники для различающихся электрических розеток, ЦОДам – очищать магистральное электричество от паразитных частот.

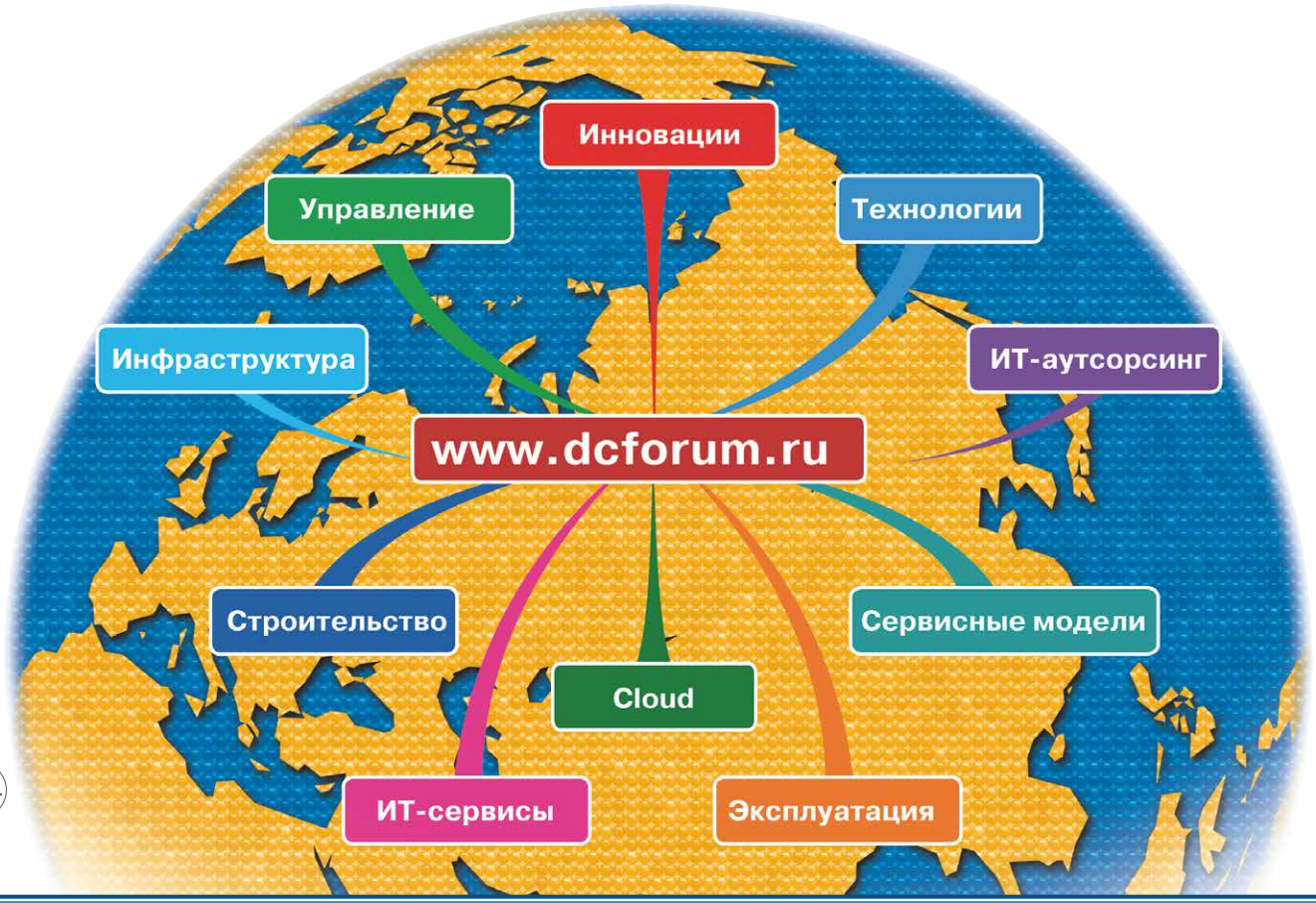
Не произойдет полной стандартизации и облачных услуг. Но тенденция к использованию общих стандартов, к возможности переноса вычислительной нагрузки с одной облачной платформы на другую, к интеграции облачных сервисов налицо. К ситуации, когда пользователь не станет задумываться, к какому облаку он подключен. Для него это будет большое облако, включающее сервисы всех провайдеров, – мультиоблако. ИКС

15-я международная конференция и выставка

ЦОД

22 сентября 2020, Москва
Конгресс-Парк отеля Radisson Collection Moscow

DATA CENTER FORUM



Реклама
16+

При поддержке

Минкомсвязь России

При участии

КООРДИНАЦИОННЫЙ СОВЕТ ПО ЦОДам И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ
Автономная некоммерческая организация

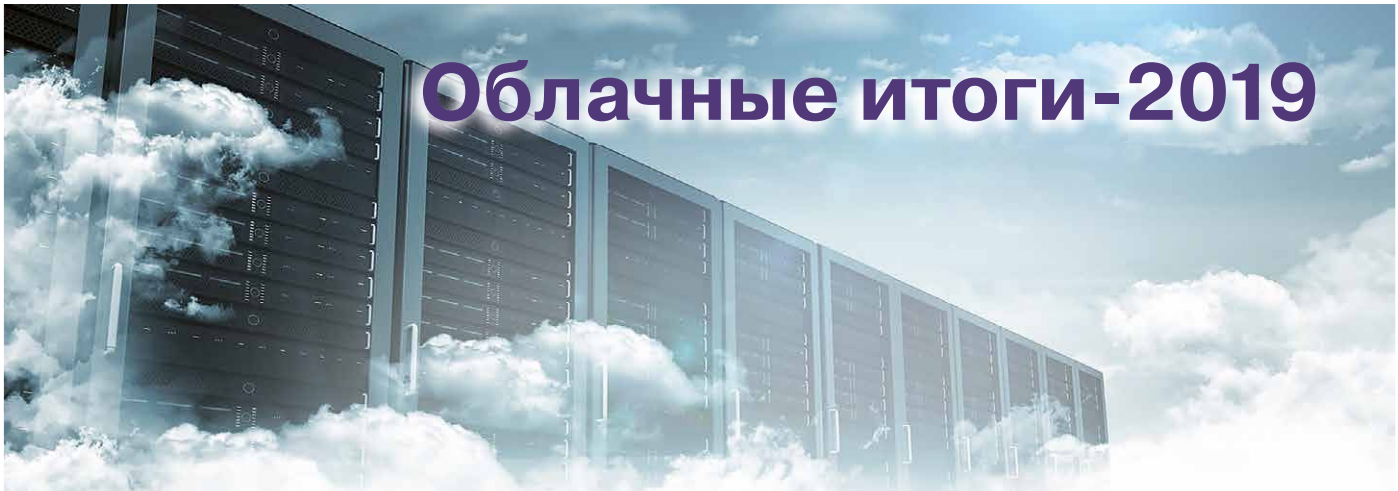
Uptime Institute

Спонсоры и партнеры

SberCloud · Life Is On Schneider Electric · HUAWEI · RITTAL · HTS · Группа Компаний ПОЖТЕХНИКА

mtu A Rolls-Royce solution · Atos · Allied Telesis · MITSUBISHI ELECTRIC Changes for the Better · ARISTA

HITEC Power Protection · C3 SOLUTIONS качественно.сделано.в России. · акционерное общество АБСОЛЮТНЫЕ ТЕХНОЛОГИИ · powerconcept BATTERY SOLUTIONS · ИМПУЛЬС источники бесперебойного питания

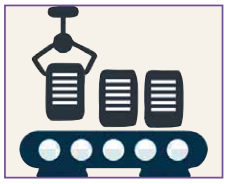


Облачные итоги-2019

Антон Салов, независимый эксперт, RCCPA

Дефицит емкостей ЦОДов, повышение активности операторов связи и самого крупного банка страны, усиление позиций китайских компаний, рост интереса к маркетплейсам – вот тенденции, проявившиеся на российском облачном рынке в 2019 г.

Отрасль ЦОДов



Первое, о чем нужно сказать, – в 2019 г. в ЦОДах Москвы образовался дефицит стойко-мест. Анонсированный в июне и введенный в эксплуатацию в октябре дата-центр IXcellerate Moscow Two фактически распродан, и британский игрок уже нацелился на скупку площадок под ЦОДы и конкурентов в московском регионе и за его пределами. После того, как было одобрено приобретение «Ростелекомом» компании DataLine, анонсированное еще в моей статье об итогах 2018 г., IXcellerate внезапно стал вторым по числу стоек игроком рынка. Стоит отметить достойную уважения модель провайдера: он фокусируется исключительно на базовых услугах ЦОДов, отдавая даже поюнитовый colocation и более верхнеуровневые услуги на откуп партнерам-клиентам. Поэтому среди его клиентов много облачных провайдеров: «Техносерв», Huawei, Tencent. У него же вторую российскую площадку открывает Servers.ru.

Несмотря на дефицит емкостей дата-центров в Москве, за МКАД еще можно найти свободные площади различного уровня – «Авантаж» (принадлежит МТС. – *Прим. ред.*), GreenBushDC, разделяющие одну площадку ЦОДы «Удомля» и «Калининский». Кстати, о последних. Много лет считалось, что ЦОД при Калининской АЭС будет коммерциализировать исключительно «Ростелеком» («РТК-ЦОД»), а «Росэнергоатом» разместит там свои стойки для собственных нужд. Однако в 2019 г. на рынок дата-центров вышел внутренний интегратор «Росатома» – «Консист-ОС». В его ближайших планах – оказание облачных услуг внешним клиентам. В основу его мультиклауда легла платформа на базе виртуализации VMware. Параллельно продолжается изучение альтернативных платформ, в том числе на основе открытых технологий. В дальнейшем планируется развернуть и услуги SaaS и тем самым составить серьезную конкуренцию соседу по площадке, у которого не заметно расширения продуктового портфеля в этом направлении. Ожидается, что новый провайдер на начальном этапе сконцентрируется на предоставлении сервисов региональным органам исполнительной власти и коммерческим клиентам из близлежащих областей. А если модель окажется успешной, то она может быть распространена на все регионы присутствия атомных электростанций «Росэнергоатома» (в том числе за пределами России). Вот тут уже действительно можно будет говорить об экспортном потенциале отрасли ЦОДов.

Операторские облака

Внезапно в рейтинге-2019 CNews по облачному провайдингу лидером рынка была названа МТС. Удивительно, оператор взломал чарты и сразу занял первое место. Бывает ли такое? Здравый смысл говорит, что нет, а эксперты ассоциации RCCPA говорят, что да, бывает. У

МТС, в отличие от соперников по пьедесталу рейтинга CNews, динамика облачной выручки вполне аудируема. Так что если верить в рейтинги, то у МТС – однозначно первое место, как минимум по темпам роста. Хотя опубликованный на полгода позже аналитический отчет iKS-Consulting отдает первое место «Ростелекому». С учетом того, что «РТК-ЦОД» и МТС появились в отчетах по облакам недавно, разночтения могут проистекать из различия методик измерений. У iKS-Consulting она более строгая, частные облака в ней не учитываются. Если лидерство МТС все же признать, то сохранить его по итогам 2019 г. компании будет сложно. Облачную выручку «Ростелекома» будут считать по группе компаний, т.е. консолидированно с DataLine, а значит, the boys are back in town!

«Мегафон» продолжает расширять партнерские продажи облака Mail.ru Cloud Solutions под своим брендом, одновременно предпринимая очередную попытку собрать собственное enterprise-облако на базе продуктов VMware. В сегменте SaaS идет неспешное развитие экосистемы ВАТС (у которой наконец-то появилось мобильное приложение!) за счет интеграции с новыми CRM. Оператор запускает их в продажу в параллель с существующим реферальным маркетплейсом для бизнеса. В конце августа «Мегафон» провел киберспортивный турнир с использованием технологий 5G и cloud gaming. В качестве платформы для облачных игр задействовалась разработка Loudplay, созданная выходцами из «МегаЛабс» и опирающаяся на инфраструктуру облака Huawei в России. Помимо этого, произошел перезапуск мобильного приложения для «МегаДиска» (облачного диска для физических лиц), готовится к перезапуску облачная ВКС.

«Вымпелком» в этом году почти не появлялся на облачных радарах, как и Tele2, которая сейчас занята объединением с «Ростелекомом».

«Сберклауд» vs «СБКлауд»

Вокруг «Сберклауда» ситуация складывалась неоднозначно. В 2018 г. Сбербанк и «Ай-Теко» договорились о создании совместной облачной платформы. Однако уже в конце года из вроде бы единого проекта сбербанковского облачного провайдера была исторгнута интеграторская ДНК в виде компании «СБКлауд». Сбербанк решил строить платформу собственными силами, сохранив при этом миноритарную долю в «СБКлауде». В итоге платформу SberCloud, основанную на технологиях виртуализации VMware, все же запустили, параллельно анонсируя, что станут продавать сервисы Amazon Web Services на территории России. В то же время сотрудники проекта воодушевленно заявляли, что уж рынок федеральных органов исполнительной власти они поделят с «Ростелекомом». Планировалось также расширить возможности платформы за счет OpenStack. Технологическая стратегия и уникальные коммерческие преимущества не были понятны ни рынку, ни самой организации. Видимо, поэтому вся вторая половина года прошла под знаком усиления команды. В нее вошли профессионалы из IBM, «Яндекс.Облака» и других профильных провайдеров/вендоров.

Однако руководство «Сберклауда», вероятно, пришло к выводу, что сильный технологический партнер им все же необходим, причем партнер с готовой платформой. Таким партнером стала Huawei. Китайскому технологическому гиганту для реализации своих облачных амбиций в России нужен стратегический партнер, который сможет привести его к бюджетам в госорганы. Традиционные партнеры Huawei, операторы связи, идут в облака своим путем, а в партнерстве с 3data слишком мало возможностей для выстраивания масштабных отношений с органами госвласти. Поэтому в Huawei, видимо, решили «не класть все яйца в одну корзину», и китайский гигант, развернув часть своего облака в ЦОДе IXcellerate, взялся помочь Сбербанку. Это стратегическое партнерство позволит «Сберклауду» успешно реализовать задачу оптимизации инфраструктурных расходов в своих дочерних и зависимых обществах, а Huawei – найти потенциальных покупателей для своих облачных технологий. (Прогноз автора полностью оправдался. В начале марта 2020 г. «Сберклауд» и Huawei объявили о стратегическом партнерстве и запуске облака SberCloud.Advanced. – *Прим. ред.*).

Главными новогодними подарками (и достижениями) для (сбер)банковского провайдера можно считать запуск собственного суперкомпьютера Christofari (№ 1 в России, № 29 в мире) и известие о том, что Сбербанк предоставит мэрии Москвы свою технологию разработки сервисов. За последней новостью стоит сложносочиненная схема доступа к ресурсам того же «Сберклауда», но через совместное предприятие. Так проще осуществлять закупки услуг и не опасаться конкуренции со стороны зрелых и голодных акул облачного рынка.

В свою очередь, «СБКлауд» в начале года вышел с идеей «франшизы по облакам», по сути, с партнерской программой white label, «уникальной для России». Компетенции и продукты у «СБклауда» хорошие – и это вселяет надежду на успех. Однако здесь, как и у ряда других про-

вайдеров с партнерской моделью, есть вероятность, что начнется внутренняя конкуренция прямых продаж и канальных, которая будет сдерживать развитие проекта. Потенциальные партнеры – системные интеграторы – просто будут бояться конкуренции со стороны «Сервионики» (ГК «Ай-Теко»).

Mail.ru vs «Яндекс»

Оба наших гиперскейлера, Mail.ru и «Яндекс», которые в прошлом году вышли на рынок, активно развивают функциональность своих платформ, хотя догнать большую тройку пока не могут – слишком мало времени прошло. И Mail.ru Cloud Solutions, и «Яндекс.Облако» демонстрируют успешные кейсы – Burger King, Ozon, Skyeng, Leroy Merlin, Lamoda и др.

Стратегии конкурентов существенно различаются: если «Яндекс.Облако» фокусируется на сервисах, самостоятельно разрабатываемых и предоставляемых на базе собственных ЦОДов, то в Mail.ru продолжают использовать внешние ЦОДы, а свое облако строят на основе OpenStack. Оба гиперскейлера успешно работают с высоконагруженными проектами, что и понятно – в этом у Mail.ru и «Яндекса» отличная экспертиза, и они готовы ею делиться. Помимо этого, они берут на аутсорсинг обучение нейросетей и коррекцию моделей.

В то же время MCS активно развивает частные облака и Managed Services (услуги управляемой инфраструктуры). Здесь публичных кейсов существенно меньше: если компании и решают отдавать в облако внутреннюю инфраструктуру, то тем, у кого это «в генах», – системным интеграторам и профессиональным ИТ-аутсорсерам. Одни из них, такие как КРОК и IBS, имеют свои ЦОДы и облака, другие нет. И вот последние – при должном подходе – могут стать потребителями инфраструктуры гиперскейлеров.

Но перевести корпоративные информационные системы с VMware на KVM/OpenStack непросто. Этой экспертизы у небольших интеграторов нет, а клиенты хотят решение «под ключ». Поэтому в массе запросов VMware прописывается жестко, даже если это дороже, и гиперскейлеры не попадают в шортлист. Таким образом, заложенная много лет назад специализация на высоконагруженных и корпоративных задачах определяет профиль потребления услуг IaaS/PaaS: российские клиенты не пытаются размещать продуктивные SAP-системы у гиперскейлеров, а высоконагруженные сайты готовить с помощью облаков от операторов или системных интеграторов. Из всего бывают исключения, но ситуация такова, и тенденция сохраняется.

Microsoft vs Amazon

Еще одно важное событие 2019 г., которое серьезно повлияло на облачный ландшафт, – это изменения в подходе к партнерскому каналу Microsoft. В начале года, после введения «налога на Google», облачные продукты Microsoft тоже стали поставляться с НДС. Восторжествовала справедливость, о которой много раз просили профильное министерство отечественные провайдеры и эксперты отрасли. Однако на этом все не закончилось. В начале весны в программе Cloud Solution Provider (CSP), по которой поставляются облачные продукты Microsoft, был введен мораторий, до завершения которого компания обещала обслуживать только существующих клиентов и партнеров CSP. Плохо для рынка? Да, но не смертельно – действующие партнеры подготовились заранее и смогли продержаться несколько месяцев, распродавая заготовленное. Однако по итогам года доходы от CSP явно не вышли на запланированные значения.

В целом 2019 г. прошел под флагом «закручивания гаек» в части комплаенса, о чем даже было заявлено со сцены TMobile Arena в Лас-Вегасе во время ключевого партнерского мероприятия Microsoft Inspire 2019. Комплаенс идет бок о бок с безопасностью, а безопасность – наше всё (и их тоже). Весной все партнеры – участники программы Open Value (порядка 2 тыс.) должны были пройти повторную авторизацию. В итоге процедуру прошли лишь несколько десятков. Некоторые именитые партнеры были лишены права продавать не только по Open Value среднему и малому бизнесу, но и по лицензии EA/EAS в сегмент enterprise.

Microsoft вполне можно понять – компания защищается от рисков, связанных с поставкой своих сервисов и ПО в санкционные компании и регионы. Но партнеры, которые не прошли авторизацию, были вынуждены срочно искать замену продуктам Microsoft, в том числе в облаках. Многие интеграторы слишком хорошо «держат» своих клиентов, поэтому убедить их мигрировать на альтернативные технологии и платформы не составит труда.

Другие глобальные американские провайдеры и производители ПО, конкурирующие с Microsoft, тоже не горят желанием попасть под санкции, а значит, от этого уже в ближайшее время начнут выигрывать европейские (в меньшей мере), китайские (в большей) и отечественные поставщики. К сожалению, от облачного

импортозамещения выигрывают пока лишь инфраструктурные игроки. Многие из тех, кому указали на необходимость приобрести импортозамещающий софт, закупают его для отчетности, кладут на полку и продолжают использовать то, что использовали. Поэтому в сегменте SaaS работа идет на перспективу. Рано или поздно усилиями наших или американских регуляторов отечественный потребитель перейдет на отечественное ПО, тем более что в SOHO и малом бизнесе подавляющее число SaaS- и BPaaS-сервисов – российские.

Amazon с конца прошлого года занялась усилением работы на российской территории путем найма менеджмента, отвечающего в том числе за Россию. Эксперты IDC связывают это с тем, что бизнес идет хорошо и потому в регион планируют инвестировать, а проактивно управлять им из Люксембурга сложно. С другой стороны, по данным отчета iKS-Consulting, вышедшего в начале года, доля рынка AWS сравнима с Azure, хотя Microsoft в России активно работала с каналом, а AWS – нет. А значит, есть потенциал, ведь рынок IaaS/PaaS неизменно растет. В команду AWS EMEA в 2019 г. перешли сильные менеджеры, которые в свое время развивали российское отделение Microsoft. Изменит ли это что-то в отношении к российскому рынку, покажет время.

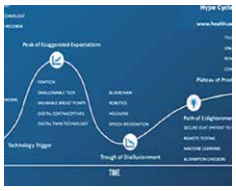
ТАРМы и рабочие места по подписке

В начале года IBS опубликовала интересный кейс, связанный с организацией виртуальных рабочих мест по технологии VDI для сотрудников компании «Гражданские самолеты Сухого». И хотя в итоге стоимость внедрения VDI оказалась сопоставимой с заменой парка ПК, кейс примечательный. Стоимость владения VDI и потери в клиентском опыте (а значит, и в производительности труда) компенсируются безопасностью и снижением риска попасть под санкции.

Та же IBS (на этот раз «ИБС Экспертиза») в ноябре выиграла подряд у Минкомсвязи на разработку технического проекта перевода госорганов на типовое автоматизированное рабочее место (ТАРМ) госслужащего. Есть вероятность, что собираться оно будет по тем же принципам VDI, хотя существуют и другие подходы, например подписка/аренда ТАРМ.

В США и Европе концепция PCaaS (Device as a Service, DaaS) активно развивается, спрос на нее растет и в малом, и в крупном бизнесе. У нас же это направление пока в начале пути. Есть вероятность, что спрос на ТАРМы в госсекторе приведет к повсеместному распространению таких услуг. Их преимущество перед VDI – в существенно лучших пользовательских характеристиках и меньшей требовательности к каналам связи, а значит, меньшей совокупной стоимости владения. Особенно логично, если эту услугу будут предоставлять операторы связи – кто, как не они, могут оценить пригодность канала связи для той или иной технологии, а если характеристики недостаточны – улучшить их. Технологической основой для ее реализации может стать KasperskyOS – операционная система для подключенных к интернету встраиваемых систем с особыми требованиями к кибербезопасности. Уже сейчас анонсирована реализация для тонких клиентов, впереди релизы для ограниченного перечня типовых ПК, а потом и версия для мобильных устройств. Многие отечественные игроки рынка импортозамещения прикладного ПО, такие как «МойОфис» и CommuniGate Pro, работают над обеспечением совместимости с этой ОС.

Тренды, маркетплейсы и инвестиционный климат



Что еще было заметного в облаках в 2019 г.? Хайп вокруг майнинга, криптовалют и блокчейна постепенно сошел на нет и ушел за горизонт кривой Gartner. О том, что технология блокчейн уже не обладает теми перспективами, о которых многие говорили несколько лет назад, и «ушла из научной повестки», заявила даже Наталья Касперская. Зато на взлет пошел спрос на роботизацию процессов (RPA).

Снова вырос интерес к маркетплейсам. Особенно это заметно на консьюмерском рынке и у банков. «Тинькофф», «Мегафон», Tele2 активно обзаводятся маркетплейсами для своих клиентов. Не отстает и Сбербанк, который более основательно подходит к этому вопросу, особенно в сегменте B2B. В конце года об аналогичной инициативе объявил ВТБ.

Стало меньше хайпа вокруг венчурных инвестиций, в том числе в облака – ФРИИ в начале года объявил, что завершил фазу активного инвестирования и занялся развитием портфельных стартапов. Уголовное дело Майкла Калви и претензии «Рамблера» к Nginx явно не добавили тепла российскому инвестиционному климату. Однако в конце года лидер российского рынка платформ BPaaS и коммуникационных PaaS компания Voximplant «подняла» раунд инвестиций от Baring Vostok и ее партнеров. Это позитивно, потому что оставляет шансы компаниям с российскими корнями, играющим на глобальных рынках. ИКС

Альтернативный «Джокер»: как технологии видеоанализа могли бы спасти Артура Флека

Сергей Полухин, руководитель направления видеоаналитики для безопасности предприятий и городов, TRASSIR

Современные интеллектуальные электронные системы способны предотвратить как обычные недоразумения, так и крупные неприятности.

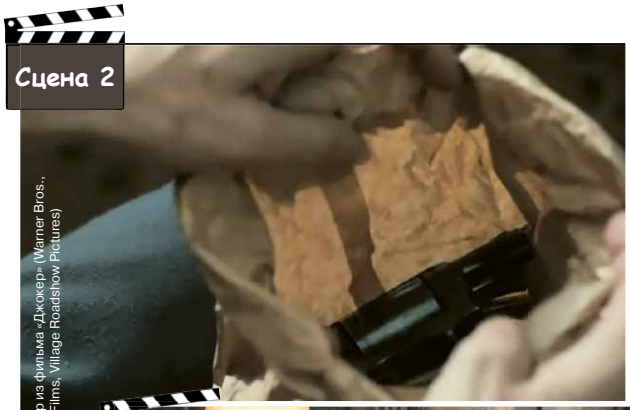
Новый фильм «Джокер», появившийся на экранах в октябре 2019 г. и претендовавший на девять «Оскаров», практически лишен спецэффектов и не похож на привычные супергеройские блокбастеры вселенной DC. У режиссера Тодда Филлипса получилась очень жизненная история, которая могла бы произойти в любом современном мегаполисе. В центре повествования – психически неуравновешенный одинокий комик-неудачник Артур Флек, который, сталкиваясь с равнодушием и жестокостью общества, постепенно сходит с ума. Неожиданно безумие Артура становится катализатором общественного взрыва, весьма болезненно прокатившегося по страдающему от социального расслоения Готэм-сити. Наблюдая за тем, как трагедия одного человека тянет за собой череду смертей и кровавых событий в масштабах целого города, невольно задаешься вопросом – можно ли было этого избежать?

Да, конечно, – скажем сразу, чтобы больше к этому не возвращаться, – Артура (и Готэм-сити) могла бы спасти дружеская поддержка или простое неравнодушие прохожих. Но в мегаполисах, где каждый сам за себя и «умные» технологии давно заменили человеческую помощь, трудно ожидать участия от незнакомых людей. А вот современные интеллектуальные электронные системы могли бы, пожалуй, повернуть сценарий «Джокера» в иное русло. Уж они-то участвуют в нашей жизни сегодня на каждом шагу. Итак, посмотрим, как с их помощью могла измениться история Артура Флека.

Кадры из фильма «Джокер» (Warner Bros., DC Films, Village Roadshow Pictures)

Подростки на улице отбирают у Артура плакат, с которым он работает, и избивают его в переулке, когда он пытается его вернуть. Именно с этого начинается ухудшение его психического состояния.

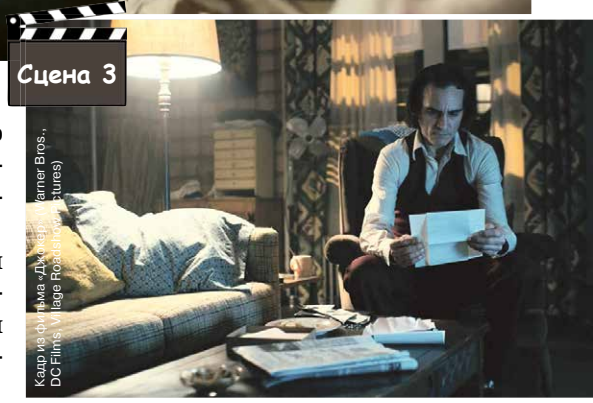
Альтернативная реальность: месяц назад в этом районе был запущен пилотный проект полицейского видеонаблюдения с «умной» обработкой видео. Камеры, проанализировав скорость и траектории передвижения людей, зафиксировали аномальную активность и отправили сигнал на пульт дежурного, который передал информацию патрульной машине. Та оказалась рядом, прибыв на место происшествия уже через три минуты, и избиения Артура не произошло – подростки испугались и убежали. Через месяц Артура приглашают в мэрию как живое подтверждение того, что система работает. Он получает внимание, в котором так нуждается.



Кадр из фильма «Джокер» (Warner Bros., DC Films, Village Roadshow Pictures)

Коллега Рэндалл одалживает Артуру пистолет. Из-за него Артур теряет работу (пистолет выпадает из кармана во время представления в детской больнице) и из него же впоследствии убивает троих напавших на него в метро молодых людей, а потом – ведущего Мюррея Франклина.

Альтернативная реальность: владелец агентства развлечений, в котором работает Артур, контролирует подчиненных с помощью видеонаблюдения. Аналитический блок системы настроен таким образом, чтобы фиксировать время, проводимое актерами в гримерной, а также распознавать потенциально опасные объекты. Когда камеры фиксируют в кадре пистолет, владельцу на телефон приходит тревожное сообщение. Он врывается в гримерку комиков и со скандалом увольняет Рендалла. Артур, не успев выдать себя, сохраняет работу.



Кадр из фильма «Джокер» (Warner Bros., DC Films, Village Roadshow Pictures)

Артур находит письмо матери Тому Уэйну, из которого узнает, что якобы он его внебрачный сын. Артур ищет встречи со своим «отцом», который обходится с ним очень жестко, и это еще сильнее дестабилизирует его состояние.

Альтернативная реальность: Пенни Флек пишет Тому по электронной почте, а на ее ноутбуке включена биометрическая идентификация – система распознавания по лицу. Поэтому попытки Артура получить доступ к почте матери ни к чему не приводят. Он остается в неведении относительно ее бредовых фантазий и не ищет встречи с Уэйном.

Кадр из фильма «Джокер» (Warner Bros., DC Films, Village Roadshow Pictures)

Артур приходит в особняк Тома Уэйна, разговаривает с его сыном, нападает на дворецкого. Дворецкий сообщает, что отцовство Уэйна – неправда.

Альтернативная реальность: Том Уэйн, получив от матери Артура два десятка писем, понимает, что имеет дело с сумасшедшей женщиной, и, желая обезопасить себя и свою семью, дает начальнику службы охраны указание настроить аналитический блок системы видеонаблюдения особняка на распознавание лица Пенни, а заодно и Артура. Предосторожность оказывается нелишней: скоро камеры действительно «узнают» в лицо пришедшего к особняку Артура. Охрана вежливо просит его удалиться, разговора с дворецким на повышенных тонах не происходит.

Кадр из фильма «Джокер» (Warner Bros., DC Films, Village Roadshow Pictures)

Артур крадет из архива больницы дело своей матери и узнает, что он – приемный сын и что в детстве он подвергался физическому насилию со стороны приемных родителей.

Альтернативная реальность: все архивы больницы оцифрованы; клерк находит дело в базе данных, но отказывается распечатать его для Артура без письменного согласия Пенни. Артур уходит ни с чем, страшная тайна остается тайной.

Артур знакомится в лифте с соседкой Софи, она проводит с ним время, приходит на его выступление в клубе, поддерживает, когда его мать госпитализируют с инфарктом. Позже оказывается, что их общение – лишь плод воображения Артура.

Альтернативная реальность: Артур и Софи обмениваются телефонами, и у них завязывается общение в мессенджере. Артур понимает, что ему гораздо проще поддерживать контакт с помощью переписки: девушка не видит его странных приступов смеха, и у него всегда есть время обдумать и сформулировать фразу. Он чувствует себя гораздо спокойнее и увереннее, общаясь онлайн. Софи, в свою очередь, находит Артура приятным собеседником. Они становятся друзьями.

Кадр из фильма «Джокер» (Warner Bros., DC Films, Village Roadshow Pictures)

Кадр из фильма «Джокер» (Warner Bros., DC Films, Village Roadshow Pictures)

Артур узнает, что город сократил финансирование соцпрограмм и что он больше не сможет приходить на регулярные встречи с социальным психологом, которая проявляла участие и контролировала его состояние, а также получать рецепты на психотропные препараты. Без таблеток нестабильное состояние Артура быстро ухудшается – он становится агрессивным.

Альтернативная реальность: город находит возможность сократить расходы в других областях, в частности, уменьшает количество полицейских машин, патрулирующих улицы ночью, – вместо них монтируют системы видеонаблюдения, которые распознают аномальную активность (драки, ограбления, кражи в магазинах, крики о помощи) и автоматически отправляют сигнал на пульт дежурного, а также включают сирену и звуковое предупреждение. Система оказывается эффективной: автоматическая сигнализация отпугивает большинство мелких преступников, а одна патрульная машина теперь справляется с работой, которую раньше выполняли пять экипажей. Высвободившиеся в городском бюджете средства перераспределяют так, чтобы социальные службы не потеряли финансирование. Артур продолжает получать препараты и сохраняет относительно стабильное психическое состояние.


Кадр из фильма «Джокер» (Warner Bros., DC Films, Village Roadshow Pictures)

Ключевое событие фильма, когда Артур убивает в метро троих напавших на него богатых парней и убегает. Свидетели дают показания, что убийства совершил человек в гриме клоуна. Неосторожное телевысказывание Тома Уэйна о предполагаемом убийце провоцирует массовое недовольство жителей города. В Готэм-сити начинаются беспорядки.

Альтернативная реальность #1: сканирующая система на входе в метро распознает пистолет и поднимает тревогу. Артур пытается убежать, но аналитический блок системы видеонаблюдения, работающий в связке со сканером, фиксирует его лицо в гриме и передает эти данные по сети, отслеживая передвижение потенциального преступника. Полицейские задерживают Артура и изымают оружие. В ходе разбирательства выясняется, что Артур невменяем, и его отправляют на принудительное лечение. Он снова получает психотропы, а трое парней, Пенни Флек и Мюррей Франклин остаются живы.

Альтернативная реальность #2: камеры слежения, установленные в вагонах метро, фиксируют действия трех богатых хулиганов и идентифицируют их как опасные (чрезмерно резкие и активные в сравнении с обычным поведением пассажиров метро). Машинист получает тревожный сигнал, вызывает полицейских на ближайшую станцию и объявляет об этом по громкой связи. Поняв, что их засекли, нападающие бросают Артура и убегают в другой вагон. Артур же, испугавшись камер и полиции, не стреляет им вслед, а прячет пистолет под сиденье. Когда поезд приезжает на станцию, полицейские забирают Артура и передают медикам. В госпитале ему оказывают помощь и назначают консультацию психиатра. Резонансное убийство не состоялось и не повлекло за собой социального взрыва.

И в кино, и в жизни

В истории Джокера много поворотных точек, и современные технологии, по всей вероятности, могли бы повлиять на каждую из них. Правда, в этом случае зрители остались бы без захватывающего фильма, кинокритики – без хвалебных рецензий, а блистательный Хоакин Феникс – без впечатляющей роли, которая принесла ему «Оскара». А вот в реальной жизни пользоваться возможностями «умных» электронных систем можно и нужно: жизнь не кино, а электроника способна предотвратить как недоразумения, так и крупные неприятности. Тем более что все описанные возможности – и куда бóльшие – в современном мире уже давно не фантазия сценариста. ИКС

5-я международная конференция и выставка

«ЦОД: модели, сервисы, инфраструктура»

11 июня 2020, Казахстан, Алматы, The Rixos Hotel Almaty

Фокус конференции:

- Рынок дата-центров и облачных сервисов Казахстана
- Транзитный и экспортный потенциал отрасли ЦОДов Казахстана
- Кибербезопасность в эпоху цифровизации
- Распределенные облака. Гибридная модель. Мультиклауд
- Как построить ЦОД быстро и качественно. Модульные и префаб-решения
- ИТ на основе открытого ПО. Риски и преимущества

При участии

КООРДИНАЦИОННЫЙ СОВЕТ ПО ЦОДам И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ
Автономная некоммерческая организация

Uptime Institute

Организаторы

ИКС МЕДИА

iKS CONSULTING

www.dcforum.kz

Реклама 16+

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

Спонсоры и партнеры

Life Is On Schneider Electric

Atos

СЭ SOLUTIONS
КАЧЕСТВЕННО.СДЕЛАНО.В РОССИИ.

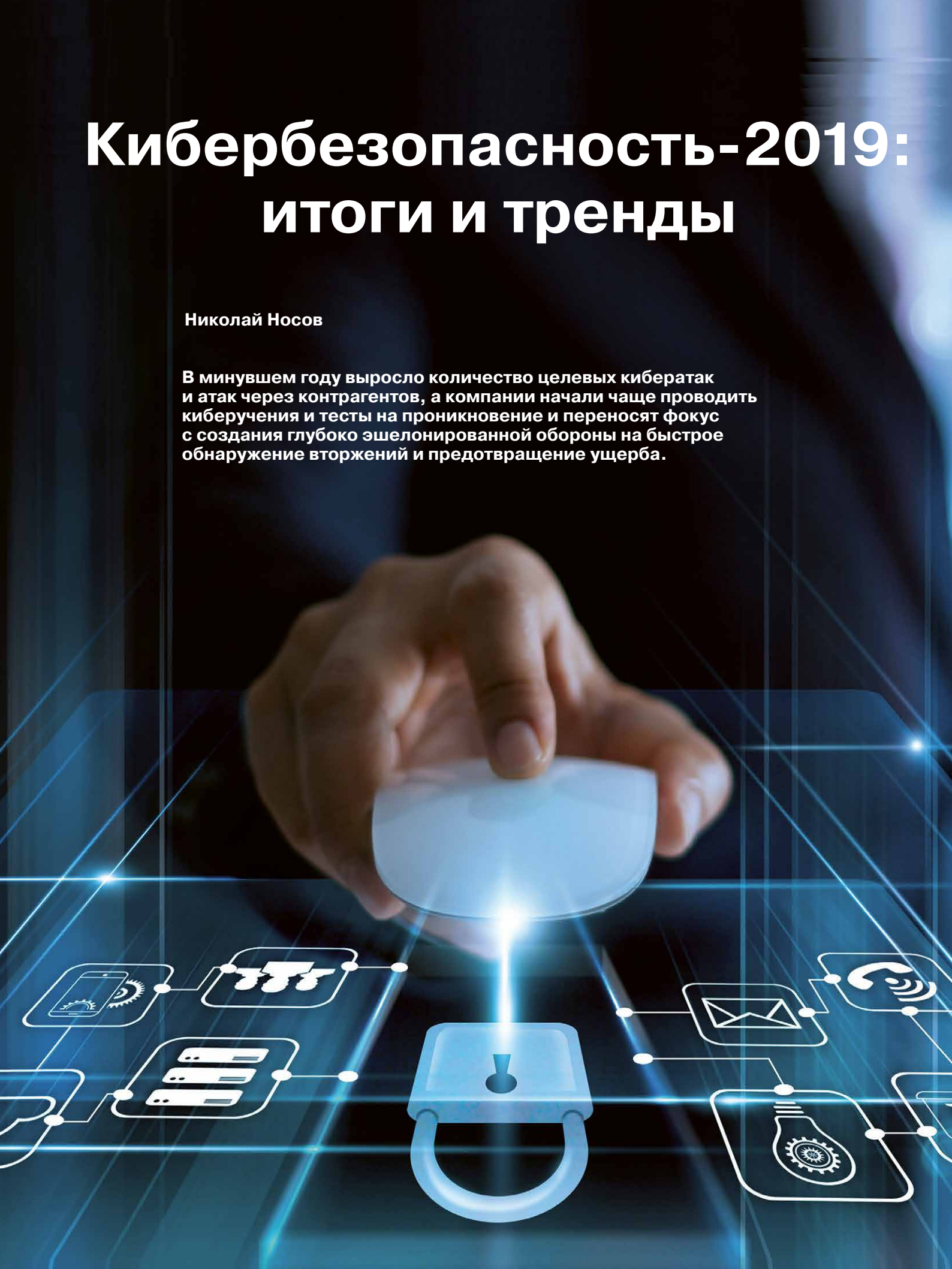
MITSUBISHI ELECTRIC
Changes for the Better

АККУ ЭНЕРГО

Кибербезопасность-2019: итоги и тренды

Николай Носов

В минувшем году выросло количество целевых кибератак и атак через контрагентов, а компании начали чаще проводить киберучения и тесты на проникновение и переносят фокус с создания глубоко эшелонированной обороны на быстрое обнаружение вторжений и предотвращение ущерба.



Состояние рынка

Российский рынок информационной безопасности в 2019 г. вырос, но этого, можно сказать, никто не заметил: бюджеты, выделяемые в компаниях на кибербезопасность, увеличились, по оценке Бориса Симиса, заместителя генерального директора по развитию бизнеса Positive Technologies, в среднем на 20%, но не были израсходованы полностью. По его мнению, это во многом обусловлено необходимостью проведения длительных конкурсных процедур, в результате чего компании не успели закупить необходимые средства защиты.

Сменилась парадигма обеспечения информационной безопасности – теперь компании не пытаются построить неприступные защитные редуты, сознавая, что это бесполезно, а ставят своей целью быстро выявить атаку и предотвратить непоправимый ущерб. В связи с этим растет потребность в высокоинтеллектуальных системах защиты с анализом трафика и управлением информацией о безопасности и событиями безопасности (SIEM), а также в комплексных APT-решениях.

Увеличился спрос на специалистов, обладающих несколькими компетенциями, например в кибербезопасности и data science, информационной безопасности и АСУ ТП. Бизнес стал понимать, что не имеет необходимого количества ИБ-специалистов нужного уровня, и начал переходить к аутсорсингу и аутстаффингу.

По данным опроса 200 генеральных директоров крупнейших компаний мира, проведенного компанией Ernst & Young, в ближайшие пятьдесят лет киберугрозы выйдут на первое место среди угроз для мировой экономики.

▲ Распространенные категории жертв (доля атакующих APT-группировок)

Действия регуляторов

Продолжились работы по формированию нормативной правовой базы в области защиты объектов критической информационной инфраструктуры (КИИ). ФСБ, традиционно отстающая в разработке нормативных документов от ФСТЭК, наконец сформулировала требования к средствам ГосСОПКА. 6 мая регулятор выпустил приказ № 196 «Об утверждении требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты». 19 июня вышли приказы № 281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты...» и № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах...». В них были сформулированы понятие ГосСОПКА и конкретные требования к ее субъектам. Причем это не рекомендации, а положения, обязательные для исполнения.

Разработкой нормативных документов занималось и экспертное сообщество. Так, в мае вышло подготовленное АРСИБ при помощи ФСТЭК пособие «Безопасность объектов критической информационной инфраструктуры организаций», подробно рассказывающее о шагах, которые должны сделать предприятия для выполнения требований ФЗ-187.

Начала складываться судебная практика по привлечению к ответственности по ст. 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей». Появились первые успешно доведенные до конца дела. Например, в октябре жительница Владивостока получила три года условно за кражу компьютерной информации, содержащей персональные данные клиентов.

По-прежнему активное влияние на рынок ИБ оказывает Центробанк. Согласно нормативным документам регулятора, с 1 января 2020 г. финансовые организации должны использовать программное обеспечение, у которого есть либо сертификат ФСТЭК, либо свидетельство о прохождении анализа уязвимостей. Вендоры банковского ПО стали выстраивать процессы жизненного цикла безопасной разработки, включающие этапы формирования требований, написания кода, тестирования, сертификации, эксплуатации и обновления. Для самописного ПО банки начали активно заказывать статический и динамический анализ кода.

Стоит отметить вступивший в силу 1 ноября 2019 г. закон о «суверенном интернете», неоднозначно воспринятый экспертным сообществом. Впервые закон обязывает коммерческие органи-

зации, в данном случае – операторов связи, проводить киберучения и оценивать возможности систем безопасности по отражению атаки. Аналогичное требование к владельцам значимых объектов КИИ появилось в нормативных документах ФСБ. 23 декабря в стране прошли учения по «суверенному интернету», в ходе которых четыре федеральных оператора связи отрабатывали 18 сценариев атак: 12 – через сети с протоколом сигнализации SS7 и шесть – через сети с протоколом DIAMETER, используемым в сетях 4G. Киберучения, проведение тестов на проникновение становятся хорошей практикой во всё большем числе компаний.

Общие тенденции инфобезопасности

Согласно исследованию компании Positive Technologies «Кибербезопасность 2019–2020: тенденции и прогнозы», в минувшем году целенаправленные атаки преобладали над массовыми: в третьем квартале их доля составила 65% (против 59% во втором квартале и 47% – в первом). Массовые атаки перестают работать, так как организации начинают применять более эффективные средства защиты. APT-группировки все чаще выбирают для атак предприятия малого и среднего бизнеса, не имеющие достаточных ресурсов для обеспечения безопасности. Взлом менее защищенных компаний позволяет проводить атаки на более защищенных контрагентов, задействуя доверенные каналы между ними.

Злоумышленники все чаще используют специализацию и сервисные модели. Одни группировки взламывают сети, другие платят за доступ и атакуют с помощью вирусов-шифровальщиков или похищают данные.

Сохраняется тенденция к размытию контура безопасности предприятия. Руководители все чаще разрешают сотрудникам использовать в бизнес-процессе смартфоны и планшеты. В повседневную жизнь вошли облачные вычисления, а взлет интереса к мультиоблакам еще больше усложняет работу специалистам по информационной безопасности.

Среди исследователей трендом стал поиск аппаратных уязвимостей. Специалисты ищут и находят уязвимости на уровне печатной платы и элементов аппаратной логики. Публичных кейсов о реальном ущербе мало, но крупные компании уже начали закладывать соответствующие риски в модель угроз и выделять бюджеты на защиту.

Рост атак на пользователей

За три квартала 2019 г. Positive Technologies насчитала 231 хакерскую кампанию, направленную на конечных пользователей (за аналогичный период 2018 г. – 217 кампаний). Основные методы атак – социальная инженерия и заражение устройств вредоносным ПО. Вдвое уменьшилась доля атак на пользователей с подбором паролей к учетным записям на сайтах, что связано с распространением двухфакторной аутентификации.

Злоумышленники активно используют уязвимости веб-сайтов. По данным Positive Technologies за 2019 г., 92% веб-приложений позволяют проводить атаки на пользователей, при этом 82% найденных уязвимостей связаны с ошибками, допущенными при разработке. Бреши безопасности в 16% исследованных сайтов давали возможность контролировать не только само веб-приложение, но и сервер.

Интерес для преступников представляют конечные устройства пользователей. Многие мобильные банковские приложения позволяют войти в них по отпечатку пальца, что удобно, но небезопасно. В октябре исследователи из X-Lab за 20 мин разблокировали смартфон, используя отпечаток пальца хозяина, взятый со стакана. При этом применялись приложение Tencent Security, способное реконструировать отпечаток даже по его фрагментам, снятым с нескольких предметов, а также гравировальный аппарат стоимостью $140. Не менее опасно использовать для входа в банковское приложение только PIN-код. В случае кражи устройства подбор PIN-кода простым перебором не займет много времени.

В мае большой резонанс вызвало сообщение Facebook о закрытии уязвимости в принадлежащем компании мессенджере WhatsApp. Для установки вредоносного ПО, позволяющего следить за пользователем, достаточно было совершить звонок на телефон жертвы.

Лидируют по-прежнему вредоносные приложения, которые пользователь устанавливает сам. Эти программы запрашивают специальные разрешения, в том числе связанные с администрированием устройства. Не спасает и установка из такого вроде бы доверенного источни-

ка, как магазин приложений. Ситуацией озаботились вендоры. В рамках запущенной в 2019 г. программы Google Play Security Rewards Program исследователи могут получить выплаты за нахождение уязвимости в любом Android-приложении с числом установок от 100 млн. Эта мера должна привести к улучшению защищенности популярных Android-приложений.

Широкое распространение получили атаки, задействующие пользовательские данные, которые крадутся у организаций и продаются в даркнете. Например, злоумышленники представляются сотрудниками банка и пытаются по телефону заставить жертву перевести им через интернет деньги с помощью личного кабинета.

Большой проблемой для пользователей в этом году стали спам-звонки, которые осуществлялись с помощью записанных рекламных объявлений, умных чат-ботов или непосредственно человека. Операторы связи начали реагировать на жалобы пользователей и предлагать приложения для проверки входящих звонков.

Растет число мошеннических операций с бесконтактной оплатой – злоумышленники располагаются рядом с жертвой и переводят с его гаджета небольшие суммы, не требующие ввода PIN-кода.

Госсектор и бизнес

Увеличивается число атак на госучреждения. За первые три квартала 2019 г. Positive Technologies зафиксировала 167 атак на госучреждения (за такой же период в 2018 г. было зафиксировано 133 атаки). Чаще всего они проходили с использованием фишинга (49% атак) и вредоносного ПО (63%). 18% атак были связаны со взломом веб-приложений (в 2018 г. этот показатель был почти таким же – 19%).

Серьезной проблемой в 2019 г. стал телефонный терроризм. Раньше телефонных террористов было легко отследить, определить место звонка и принять меры. Сейчас злоумышленники покупают доступ к IP-телефонии за рубежом и, пользуясь подменой номеров, звонят и сообщают о минировании государственного объекта, магазина, школы или детского сада. Атака происходит из-за пределов страны, расследование требует долгого и далеко не всегда простого взаимодействия со службами других государств, зачастую не имеющих желания заниматься нашими проблемами.

Растет интерес киберпреступников к промышленному сектору. Широкую огласку получило нападение на Norsk Hydro. Ущерб от атаки на норвежского производителя алюминия был оценен в $41 млн. Задействованный тогда шифровальщик LockerGoga использовался и в атаках на три химические компании США. В июне 2019 г. атака шифровальщика-вымогателя частично парализовала производство бельгийской компании ASCO Industries, крупного поставщика авиационных компонентов. В целом за три квартала 2019 г. Positive Technologies зафиксировала 92 кибератаки на промышленные объекты, что существенно превышает показатель аналогичного периода 2018 г. (25 атак).

Немного меньше стали атаковать финансовые учреждения, прежде всего за счет снижения доли массовых атак. «В третьем квартале 2019 г. всего 4% зафиксированных атак носили массовый характер, а в аналогичный период годом ранее этот показатель был на уровне 32%», – пояснил руководитель группы исследований безопасности банковских систем Positive Technologies Ярослав Бабин. При этом число целенаправленных атак на финансовые организации не уменьшается. Три из десяти выявленных APT-группировок внедряют вредоносное ПО в инфраструктуру банков через профильные ресурсы, посещаемые сотрудниками финансового учреждения, три – взламывают менее защищенную инфраструктуру компаний-партнеров или филиалов, у которых есть легитимные каналы в целевую финансовую организацию.

DDoS-атаки растут количественно и качественно

«По нашим оценкам, общее количество распределенных атак, направленных на отказ в обслуживании (Distributed Denial of Service, DDoS), за 2019 г. выросло примерно в полтора раза», – констатировал технический директор компании Qrator Labs Артем Гавриченков. Наиболее атакуемые индустрии – платежные системы, электронная коммерция и беттинг (ставки на исход спортивных матчей и иных событий). Банки теряют свою привлекательность для преступников благодаря широкому применению средств защиты, хотя число DDoS-атак на них по-прежнему велико. Лидерами по росту числа атак стали платежные системы (+187%) и криптосервисы (+487%).

В 2019 г. были выявлены новые типы DDoS-атак с использованием техники amplification («усиление», когда атакующий от имени жертвы

Источник: Qrator Labs

▲ Наиболее страдающие от DDoS-атак отрасли

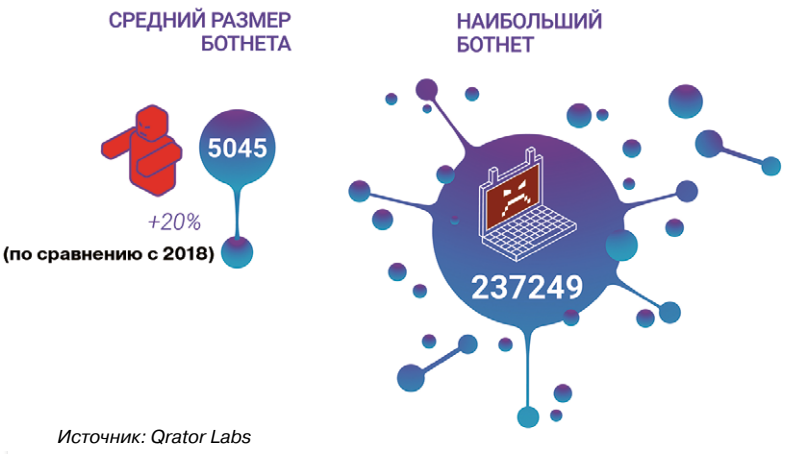
отправляет поддельный запрос, в ответ на который жертва получает значительно большее количество данных и вынуждена потом разгребать образовавшиеся завалы). Такие распределенные атаки, направленные на отказ в обслуживании, проводят, как сообщалось, даже школьники. Но в минувшем году были зафиксированы атаки на основе TCP-амплификации (реплицированный SYN/ACK-флуд). Возможность задействования протокола TCP для проведения масштабных атак типа amplification впервые была описана в исследовательской работе немецких ученых пять лет назад, но до прошлого года оставалась лишь теоретической.

Атаки с запросами на подключение по протоколу TCP привели в августе 2019 г. к недоступности ряда хостингов по всему миру. Трафик амплификации SYN/ACK достигал пиковых значений в 208 млн пакетов в секунду, а наиболее длительный период атаки с непрерывной бомбардировкой «мусорным» трафиком составил 11,5 ч.

При таких атаках метод защиты путем сброса всего UDP-трафика, который позволяет справиться с большей частью атак с использованием амплификации, часто не помогает нейтрализовать вектор SYN-ACK. Требуются комплексные меры защиты, которые небольшим интернет-компаниям реализовать нелегко.

Другие новые способы организации DDoS-атаки, появившиеся в 2019 г.: эксплуатация уязвимости в Web.Services.Discovery и сервисе удаленного управления компьютерами Apple (Apple ARMS), позволившая достигнуть коэффициента амплификации 35,5.

Рост размеров ботнета ▼



Источник: Qrator Labs

DDOS-атаки можно разделить на три класса. Атаки нижнего уровня (L2–L3 модели OSI) осуществляются за счет исчерпания полосы пропускания. Если представить канал как водопроводную трубу, пропускающую ограниченное количество воды, то труба забивается злоумышленником. На среднем уровне (L4–L6) атакуются криптографические и транспортные протоколы, создаются проблемы в инфраструктуре, часть узлов которой даже не контролируется оператором связи (СОРМ). На высоком уровне (L7) организуются узкие места в сайтах, платежных системах и мобильных приложениях.

Чаще атакуют нижний и верхний уровень, подобно тому, как в многоквартирном доме самые обворовываемые этажи – первый и последний. Особенность прошедшего года – рост DDoS-атак на СМИ, сайты которых нередко имеют слабую защиту от этого вида угроз. Причем атаки идут преимущественно на высоком уровне (L7).

Все больше устройств под чужим контролем

Средний размер управляемой преступниками сети (ботнета) вырос на 20%. Во многом это обусловлено использованием устройств с необновляемым ПО, например старых мобильных телефонов, и с распространением интернета вещей.

Так, недавно сообщалось об обнаружении встроенного бэкдора в платах, программируемых китайской компанией Xiongmai, которые многие бренды устанавливают в системах видеонаблюдения. В такой системе удаленный доступ к видеорегистратору можно получить, подключившись через интернет с помощью логина root и одного из шести опубликованных паролей. Программа организации DDoS-атаки, эксплуатирующей этот бэкдор, выложена на GitHub. Как правило, компании объясняют такие уязвимости халатностью разработчиков, забывших убрать фрагменты отладочного кода.

Что делать?

Новые технологии несут новые риски, а интеграция технологий только увеличивает количество векторов атак. Эксперты все чаще говорят о необходимости разрабатывать принципиально новые подходы к обеспечению кибербезопасности, но пока методы защиты радикально не изменились. Компаниям предлагают своевременно обновлять программное обеспечение, закрывая выявленные уязвимости, проводить тренинги персонала, вкладываться в современные средства защиты. Следует понимать, что главное – не закрыться от всех угроз, а вовремя выявить атаку и сделать ее менее привлекательной для злоумышленника, который тоже ищет баланс между выгодой и затраченными ресурсами. ИКС

Укрепляем обороноспособность на цифровом поле боя: делай раз, делай два, делай три

В цифровой среде обеспечение информационной безопасности становится все более актуальной задачей. Какие шаги предпринять, чтобы создаваемая система защиты информации была эффективной?

Антон Грецкий, архитектор информационной безопасности, ActiveCloud

Угрозы сегодня могут исходить отовсюду. Мобильность, облака, интернет вещей – это, с одной стороны, технологии, которые позволяют развивать бизнес, с другой – новые вызовы для служб ИБ. Не стоит сбрасывать со счетов и целевые атаки, разработанные в расчете на конкретную организацию или группу организаций, объединенных по каким-либо признакам. Такие атаки встречаются достаточно часто, и их трудно обнаружить при помощи стандартных средств защиты, которые обычно не способны эффективно бороться с подобными угрозами. Ну и наконец, источником угроз является современная сложная сеть, охватывающая большое количество филиалов и устройств и подразумевающая применение виртуализации и других технологий, которые создают определенные проблемы в обеспечении информационной безопасности.

Бизнес продолжает терять репутацию, клиентов и деньги

Если взглянуть на то, что происходит сегодня в компаниях в отношении защиты информации, мы увидим печальную картину – несмотря на увеличение затрат, инцидентов становится все больше и ущерб от них все катастрофичнее. $534 млн – такую сумму в прошлом году потеряла японская криптобиржа в результате компрометации данных ее клиентов.

Конфиденциальность, целостность и доступность своих активов большинство компаний не обеспечило до сих пор. Почему? Удивительно, но они просто не знают, что и как нужно защищать... Именно поэтому хочется еще раз обсудить, о чем нужно помнить, создавая эффективную систему защиты информации.

Начнем с аудита

А что, собственно, защищаем? Инвентаризация активов – с этого начинается построение любой системы защиты информации. Составьте перечень активов, определите их владельцев – кому в компании они нужны, кто на них зарабатывает, насколько эти активы критичны для бизнеса. Таким образом вам

удастся сформировать перечень объектов защиты.

Второй вопрос: от чего защищаем? Важным этапом работ является разработка модели угроз. Эта модель должна учитывать специфику конкретного бизнеса, условия эксплуатации активов, компетенции работников, кадровую политику, взаимоотношения с партнерами и конкурентами – мелочей здесь нет.

Оцениваем риски

Но как бизнесу понять, произойдет ли такая «неприятность» с ним и стоит ли вкладывать в ИБ деньги? Для этого вам необходимо провести оценку рисков. Именно понимание бизнесом соотношения «потери в случае реализации риска/затраты на систему защиты информации» позволит разговаривать с ним на одном языке.

Оценка рисков – это по сути определение показателей СВР (степень вероятности реализации) и СТП (степень тяжести последствий) для каждой из угроз разработанной модели. Чем выше СВР и СТП угрозы, тем выше риски для бизнеса и тем легче руководству компании принять решение об инвестициях в информационную безопасность. Все оценки ложатся в карту рисков, которая в дальнейшем будет главным инструментом по управлению этими самыми рисками.

Обосновываем список средств защиты

Проведя оценку рисков, вы сможете на основании полученных данных (финансовых и репутационных потерь в случае реализации тех или иных рисков) сформулировать задачи, которые должна решать ваша система защиты информации, составить перечень необходимых средств защиты и экономически его обосновать.

Помните, что информационная безопасность работает на бизнес, а не наоборот. И эффективная система защиты информации не должна быть избыточной, а ее масштабирование и развитие – всегда результат появления новых угроз, рисков и, как следствие, задач безопасности.

В сухом остатке

Итогом проведенных работ будут:

- реестр информационных активов компании;
- перечень угроз;
- карта рисков;
- перечень задач информационной безопасности;
- спецификация технических и организационных мер по обеспечению информационной безопасности организации;
- перечень ресурсов, необходимых для реализации проекта по информационной безопасности (время, финансы, компетенции).

Самый важный ресурс – компетенции. На данном этапе важно понять, какие компетенции в вашей организации есть, а каких решительно не хватает, чтобы сразу начать поиск недостающих. Во-первых, компетентных специалистов найти не так просто. Во-вторых, пока их нет, все ваши современные средства защиты «из правого верхнего угла квадрата Гартнера» лежат мертвым грузом, а с ними и деньги, которые в них были вложены. А деньги, как известно, должны работать.

Работу по аудиту системы безопасности вы можете провести сами или нанять аудиторскую компанию, которая все сделает за вас. Если компания с именем и опытом именно в сфере вашего бизнеса, а вы только задумались о построении или модернизации своей системы ИБ, то, возможно, для вас это лучший вариант.

Есть несколько видов аудита:

- предпроектный аудит при модернизации или построении системы защиты информации;
- аудит на соответствие требованиям стандартов;
- активный аудит – при расследовании инцидентов.

Выбор варианта аудита зависит от того, какие задачи стоят перед создаваемой системой защиты информации: должна ли она соответствовать лучшим мировым практикам или определенному перечню отраслевых стандартов.

Обязательные оргвопросы

Следующим этапом является проектирование системы защиты информации. Необходимая его часть – создание политики информационной безопасности и сопутствующих политик и регламентов, которые описывают все процессы, связанные с защитой информации, определяют ответственных за их исполнение, сроки и порядок действий, контрольные процедуры и таким образом формируют систему управления ИБ в организации. Именно на этом этапе умирают, не успев родиться, системы защиты информации многих организаций, а стопки никому не нужной бумаги ложатся в стол. Для того чтобы этого не произошло с вашей системой ИБ, обязательно сделайте несколько простых, но важных и не формальных шагов.

Разработайте политику информационной безопасности и определите в ней задачи по обеспечению ИБ, перечень ресурсов, выделяемых организацией для исполнения поставленных задач, а также роль руководства организации и

вовлеченность его в процесс обеспечения информационной безопасности. На основании этого документа строится дальнейшая стратегия развития системы ИБ в компании.

Разработайте частные политики по отдельным компонентам обеспечения ИБ, таким как антивирусная защита, резервное копирование, управление учетными записями, использование паролей, реагирование на инциденты, контроль над функционированием информационных систем организации, сбор информации об инцидентах ИБ, использование съемных носителей информации. Этот перечень не является исчерпывающим. В каждом конкретном случае он зависит от особенностей бизнес-процессов отдельно взятой компании.

Суть этих документов в том, чтобы все поставленные в них задачи исполнялись с использованием доступных ресурсов, носили регулярный характер, анализировались и являлись фундаментом для дальнейшего улучшения и развития системы ИБ, обеспечивая ее полный жизненный цикл. По итогам анализа политики должны актуализироваться, поддерживая систему ИБ в боеспособном состоянии. Обязанности по обеспечению информационной безопасности должны быть внесены в должностные инструкции ответственных за это работников, а руководство должно контролировать исполнение этих инструкций. Без этого комплекса организационных мер все купленные вами технические средства защиты останутся бесполезным железом.

Предупреждаем угрозы инсайдерства

Важное звено функционирования системы ИБ – процедура найма и увольнения работников. Известен инцидент, который произошел в американской компании Lucchese Bootmaker. Уволенный инженер воспользовался созданной ранее учетной записью, замаскированной под принтер, чтобы получить удаленный доступ к информационной системе предприятия. Он отключил почтовый сервер и сервер, который отвечал за обработку заказов и производственные процессы. При этом он удалил системные файлы, из-за чего штатным ИТ-специалистам не удалось перезагрузить систему и восстановить работу сервера. Кроме того, он заблокировал доступ к учетным записям работников, задав новые пароли. В результате инцидента производство остановилось. Руководство было вынуждено отправить по домам 300 работников. Полдня сотрудники не могли оформлять и рассылать заказы. На восстановление работы серверов подрядчикам потребовалось несколько часов, а чтобы вернуться к нормальному производственному циклу – несколько недель.

Контроль лояльности сотрудников, «мягкие» увольнения и наем работников, не имеющих в своем «активе» инцидентов, аналогичных описанному выше, позволят снизить риск возникновения цифровых угроз.

Учиться, учиться и еще раз учиться основам ИБ

Последним по счету, но не по важности идет обучение работников компании в сфере информационной безопасности. Помните о том, что самое слабое звено в любой системе ИБ – человек. Именно он по незнанию совершает действия, которые пробивают бреши в вашей защите. Обучите сотрудников безопасной работе в интернете, с электронной почтой, паролями и флешками, расскажите им, что такое фишинг и почему нельзя открывать письма от неизвестных отправителей, как обращаться с информацией ограниченного распространения и коммерческой тайной. Потраченные деньги вернутся сторицей. Периодичность такого обучения может быть разной, главное – поддерживайте знания персонала в актуальном состоянии.

Для проверки системы защиты информации создайте тестовый стенд и воспользуйтесь услугами компаний, которые проводят испытания на проникновение. На данном этапе важно понять, что не было учтено в процессе проектирования, какие угрозы не были замечены, насколько хорошо обучены ваши работники (социальная инженерия), насколько оперативно вы готовы реагировать на атаки. Это даст вам возможность доработать вашу систему защиты информации, а вашим работникам – бесценный опыт.

Plan-do-check-act

Помните: залог эффективной системы защиты информации – цикл Деминга «планирование – действие – проверка – корректировка». Все процессы обеспечения информационной безопасности, которые вы заложили в политики, должны исполняться. При этом вы должны постоянно анализировать результаты исполнения всех процессов на предмет их достаточности, эффективности и актуальности для вашего бизнеса и в случае необходимости вносить корректировки.

Выполняйте эти простые рекомендации, и вашему бизнесу будет гораздо безопаснее в современных жестоких цифровых реалиях. ИКС

Сверхкомпактный настенный шкаф для edge-приложений

Компания Schneider Electric представила сверхкомпактный 6U-микроЦОД EcoStruxure в настенном исполнении. За основу решения взят шкаф AR106VI, недавно пополнивший линейку NetShelter WX. Вертикальная компоновка шкафа дает возможность разместить на стене несколько серверов глубиной до 760 мм в формфакторе менее громоздком, чем традиционные настенные шкафы, и не занимать место на полу. Однако опционально шкаф можно установить на ролики на полу, что облегчит его перемещение, если требуется мобильность, но и в этом случае экономия занимаемой площади достигает 60%. Шкаф также поддерживает возможность вертикальной стыковки, что позволяет при необходимости увеличить количество монтажных позиций.

Базовая комплектация включает перфорированную фронтальную панель с фильтрующим элементом и заднюю панель с активной системой отведения теплоизбытков, благодаря чему шкаф можно использовать в широком диапазоне условий. Противоударная упаковка обеспечивает возможность перевозки внутри шкафа предварительно интегрированного оборудования, сборка и настройка которого осуществлялась централизованно. Нагрузочная способность шкафа –113 кг.

AR106VI совместим с широкой гаммой ИБП APC by Schneider Electric, в том числе с литий-ионными батареями. Кроме базовой защиты от воздействия окружающей среды AR106VI предоставляет расширенный функционал для удаленного мониторинга окружающей среды, доступа и видеонаблюдения посредством интеграции с NetBotz.

Schneider Electric предлагает несколько типовых конфигураций микроЦОДов для установки оборудования различной мощности с возможностью как базового мониторинга, реализованного в ИБП, так и централизованного облачного мониторинга средствами EcoStruxure IT Expert/Asset Advisor.

www.schneider-electric.ru

Бездизельная платформа ИБП для дата-центров

Компания Piller Power Systems анонсировала серию UB-V – бездизельную платформу ИБП для центров обработки данных, представляющую собой альтернативу параллельному включению нескольких статических ИБП.

Серия UB-V, в основе которой лежит система UNIBLOCK пятого поколения, включает в себя модели ИБП мощностью от 1000 до 3240 кВт, которые имеют КПД 98% при нагрузке 100% и 97% при нагрузке 50% (IEC 62040-3).

В случае кратковременных пропаданий внешней сети или при изменениях напряжения сети сверх допустимых значений автономность работы нагрузки обеспечивается за счет динамического накопителя энергии или аккумуляторных батарей (возможно использование как VRLA-, так и литий-ионных АКБ). Если сеть пропадает на длительное время, то дальнейшая бесперебойная работа продолжается от внешних ДГУ, подключаемых электрическим способом.

Существуют версии на 400 В, 690 В и 6–30 кВ. ИБП UB-V подходят для стабилизации сетей как с автономной генерацией, так и с генерацией из возобновляемых источников энергии, пригодны для поставки пиковых мощностей.

ИБП оснащены системой управления PillerLINK с функцией интеллектуальной самодиагностики. Эти ИБП отличаются нулевым временем простоя, благодаря чему не требуют отключения для технического обслуживания. Занимаемая ими площадь на 20% меньше, чем у конкурентных ИБП/ДИБП.

На сегодня самые большие моноблочные ИБП в модельном ряду Piller серии UB-V – это установки мощностью 3000 кВА/2700 кВт и 3600 кВА/3240 кВт, которые позволяют защищать нагрузки единичной мощности до 3,2 МВт.

ИБП серии UB-V будут доступны для заказа с ноября 2020 г.

www.piller.com

Адаптер для интеграции холодильных агрегатов с интернетом вещей

Компания Rittal выпустила специальный адаптер для подключения холодильных агрегатов линейки Blue e к интеллектуальным системам мониторинга и IoT-системам.

С помощью адаптера можно контролировать состояние до 10 холодильных агрегатов, подключенных по схеме master/slave. Помимо сбора данных, можно проводить анализ эффективности используемого решения для охлаждения, отслеживать неисправности и превышение предельных значений эксплуатационных параметров, а также автоматически рассылать оповещения. Все это обеспечивает более высокий уровень эксплуатационной доступности оборудования и предотвращает дорогостоящие простои.

Новый адаптер подходит для всех устройств серии Blue e, работающих с e-комфортным контроллером, – как настенных, так и потолочных холодильных агрегатов в различных исполнениях: стандартных и из нержавеющей стали. Охлаждающие устройства Rittal Nema 3R/4 и Nema 4X также легко интегрируются с IoT-системами. Их можно размещать на улице, поэтому они часто используются в установках альтернативной энергетики (солнечной или ветряной). А поскольку такие установки, как правило, находятся в удаленных местностях, необходим дистанционный мониторинг управляющих и распределительных систем.

Благодаря веб-серверу, интегрированному в IoT-интерфейс, настройка и ввод в эксплуатацию подключенного к адаптеру оборудования осуществляются без дополнительного программирования.

www.rittal.ru

Эмулятор 5G-каналов

Компания Keysight Technologies выпустила PROPSIM FS16 – решение для эмуляции каналов 5G, которое обеспечивает эффективную проверку функционирования устройств 5G New Radio с поддержкой сверхширокых полос пропускания в миллиметровом диапазоне частот, а также технологий формирования луча и конфигураций с использованием большого количества антенн.

Модель PROPSIM FS16 позволяет производителям составных микросхем и устройств 5G тестировать реальные параметры работы 5G-систем благодаря использованию технологий MIMO и Massive MIMO для приложений с большими объемами передаваемых данных. Решение реализовано на базе компактного и модульного настольного эмулятора радиочастотных каналов 5G New Radio с масштабируемой функцией затухания и интуитивно понятными программными инструментами.

Эмулятор PROPSIM FS16 поддерживает диапазон частот и полос 5G New Radio в соответствии с требованиями 3GPP.

Масштабируемый набор каналов с конфигурируемым ослаблением (от 2 до 1024) дает возможность проводить испытания широкого ряда MIMO-систем.

Решение поддерживает функцию двустороннего затухания для проверки соединения абонента с магистральным узлом связи в обоих направлениях.

Функция односторонней передачи в канале позволяет исследовать параметры затухания при передаче сигнала от узла к абоненту, способствуя повышению эффективности испытаний параметров приемника. Это обеспечивает экономичность комплексных испытаний MIMO-систем в эфирных тестовых средах согласно требованиям 3GPP.

Предложенное решение дополняет семейство эмуляторов 5G-каналов и полностью интегрируется с другими решениями Keysight для эмуляции сетей 5G.

www.keysight.com

ПЕРЕЧЕНЬ ПУБЛИКАЦИЙ-2019

КОЛОНКА РЕДАКТОРА / № 1–4

ИКС-ПАНОРАМА / № 1–4

ЭКОНОМИКА И БИЗНЕС / № 1–4

ИНФРАСТРУКТУРА / № 1–4

СЕРВИСЫ И ПРИЛОЖЕНИЯ / № 1–4

БЕЗОПАСНОСТЬ / № 1–4

3DATA
Тел.: (800) 505-1800
E-mail: 3data@3data.ru
www.3data.ru ..... 4-я обл.

АБСОЛЮТНЫЕ ТЕХНОЛОГИИ
Тел/факс: (495) 234-9888
Email: info@absolutech.ru
www.absolutech.ru ..... с. 56

POWERCOM
Тел: (495) 651-6281
Факс: (495) 651-6282
Email: sales@pcm.ru
www.pcm.ru .....с. 46

SCHNEIDER ELECTRIC
Тел.: (495) 777-9990
Факс: (495) 777-9992
www.schneider-electric.com . .1-я обл., с. 34

Указатель фирм и организаций

Учредители журнала «ИнформКурьер-Связь»:

ООО «ИКС-Медиа»:
105066, Москва
ул. Новорязанская, д. 31/7, корп. 14;
тел.: (495) 150-6424

МНТОРЭС им. А.С. Попова:
107031, Москва, ул. Рождественка,
д. 6/9/20, стр. 1;
тел.: (495) 921-1616.

8-я международная конференция

DATA CENTER DESIGN & ENGINEERING

21 мая 2020 • Москва • Центр Digital October

www.dcdeforum.ru

За дополнительной информацией обращайтесь по телефону: (495) 150-6424 и e-mail: dim@iksmedia.ru

Реклама 16+

При поддержке

Минкомсвязь России

При участии

КООРДИНАЦИОННЫЙ СОВЕТ ПО ЦОДам И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ
Автономная некоммерческая организация

Uptime Institute

Спонсоры и партнеры

Life Is On Schneider Electric

MITSUBISHI ELECTRIC
Changes for the Better

VERTIV

RITTAL

ЗЕВС ЭЛЕКТРО

Janitza

C3 SOLUTIONS
КАЧЕСТВЕННО.СДЕЛАНО.В РОССИИ.

CONTEG
to complete your network

АККУ-ФЕРТРИБ

ИМПУЛЬС
ИСТОЧНИКИ БЕСПЕРЕБОЙНОГО ПИТАНИЯ

3data Premium Data Centers

DIGITAL YARD

Цифровые дворы Цифровой экономики

Сетевые дата-центры 3data
Уровня надежности Tier-3

ММТХ
Международные магистральные телеком хабы

Дизайнерские IT-офисы
Коворкинг, ландшафтный парк

Облачные сервисы
OpenStack, IaaS, PaaS, SaaS, Cloud Storage

DC Camping, DCaaS
Аренда и размещение модульных ЦОД

Реклама

+7 (495/499) 800 1 800

3data.ru

facebook.com/dc3data