

ТЕМА НОМЕРА

ЦОДЫ И ОБЛАКА: ТРУДНОСТИ И НАДЕЖДЫ

ЦОДы Центральной Азии	7	Охлаждаем майнинговый ЦОД	32
Сколько стоит ЦОД	24	Устойчивость облаков	62

ИнформКурьер-Связь

ИКС

издается с 1992 года



Навстречу всем ветрам с IXcellerate

МЕРОПРИЯТИЯ ИКС-МЕДИА

ИКС
МЕДИА

2023

CLOUD & CONNECTIVITY 21.03
ЦОД: модели,
сервисы, инфраструктура

Data Center Design & Engineering 23.05
DC AWARDS 2023 15.06
ЦОД 2023 12.09

Eurasian Data Center & Cloud Forum 03.10
Data Center & Cloud Kazakhstan 24.10

Реклама/16+

География:

Москва
Санкт-Петербург
Казань
Екатеринбург
Ташкент
Алматы

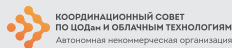


подробнее
на сайте iksmedia.ru

Издается с мая 1992 г.

Издатель
ООО «ИКС-МЕДИА»

участник
АНО КС ЦОД



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

Учредитель:
ООО «ИКС-МЕДИА»

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

РЕДАКЦИЯ
iks@iksmedia.ru

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

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

Корректор
Е.А. Краснушкина

Дизайн и верстка
Е.В. Денисова

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

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

Журнал «ИнформКурьер-Связь» зарегистрирован в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций, регистрационный номер ПИ № ФС77-82469 от 30 декабря 2021 г. Мнения авторов не всегда отражают точку зрения редакции. Статьи с пометкой «бизнес-партнер» публикуются на правах рекламы. За содержание рекламных публикаций и объявлений редакция ответственности не несет. Любое использование материалов журнала допускается только с письменного разрешения редакции и со ссылкой на журнал. Рукописи не рецензируются и не возвращаются.

© «ИнформКурьер-Связь», 2022

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

Дата подписания в печать: 03.11.22.
Дата выхода в свет: 15.11.22.
Тираж 5 000 экз. Свободная цена.
Формат 64x84/8
Типография: ООО «ПРОПЕЧАТЬ»,
адрес типографии 119618, г. Москва,
Боровское ш., дом 2А, корп. 4, кв. 260.

ISSN 0869-7973

Восходящий рынок Центральной Азии



Люблю командировки в Казахстан и Узбекистан осенью, когда «ИКС-Медиа» традиционно проводит там конференции по ЦОДам и облачным сервисам. Это возможность вырваться из уже затянутой серыми тучами промозглой Москвы, насладиться теплым солнцем и столь же теплой атмосферой мероприятий, пообщаться с необычайно доброжелательными людьми. Модерировать конференции там – одно удовольствие: делегаты жадно впитывают каждое слово выступающих, нет столичных снобов, своим видом показывающих, что знают больше всех.

В этом году меня поразили несколько фактов. В Узбекистане, где рынок коммерческих ЦОДов насчитывает лишь сотню с небольшим стоек, строится объект на 2000 стойко-мест. А Казахстан в недавно опубликованном рейтинге ООН, отражающем электронное участие граждан во взаимодействии с государством (E-Participation Index), занял 15-е место – тогда как Россия только 57-е, на две позиции позади Узбекистана. Приятно удивило, что представитель профильного министерства (руководитель Управления развития новых технологий и инфраструктуры в области связи Министерства цифрового развития, инноваций и аэрокосмической промышленности РК) весь день работал на конференции, внимательно слушал, задавал вопросы.

И с технологиями в Казахстане и Узбекистане все в порядке. Например, в получившем сертификат Tier III Facility новом ЦОДе «Казтелепорта» применяются литий-ионные батареи, а его расчетный коэффициент энергоэффективности (PUE) меньше 1,2, что существенно лучше среднего показателя по отрасли. Даже завидно, что коллегам доступны самые современные мировые технические решения, о которым нам остается разве что писать статьи.

Центральная Азия впитывает российский опыт и наилучшие практики, а теперь и наших специалистов. В кулуарах представитель одного из казахстанских ЦОДов не скрывал радости, что ему удалось заполучить несколько российских профи по эксплуатации – раньше они были финансово недоступны, а теперь готовы работать «за жилье и еду».

Что же, как бы ни было обидно, у России свой особый путь. Остается надеяться, что, пройдя его, мы потеряем (специалистов, экспертизы, технологий...) меньше, чем приобретем (технологическую независимость, собственную отрасль цодостроения...). Как показывает история, в самые тяжелые времена Россия достигала наиболее впечатляющих результатов.

С верой в российскую отрасль ЦОДов,
Александр Барсков

ЦОДы и облака: трудности и надежды

с. 58

1 КОЛОНКА РЕДАКТОРА

4 ИКС-Панорама

- 4 Рынок ЦОДов: рост на фоне спада
- 7 Готовы к рывку
- 10 Казахстан задает цифровую моду
- 13 ДАЙДЖЕСТ ОТРАСЛИ ЦОДов

14 Экономика и бизнес

- 14 И. Бакланов. О дивный старый мир!
- 17 Н. Носов. Цифровой рубль становится ближе
- 20 К. Чеханков. ИТ-трансформация бизнеса: выстраиваем процесс правильно

24 Инфраструктура

- 24 А. Павлов. От чего зависит стоимость проектирования и строительства ЦОДа?
- 28 С. Вышемирский. Как строить ЦОДы в условиях санкций



Казахстан задает
цифровую моду

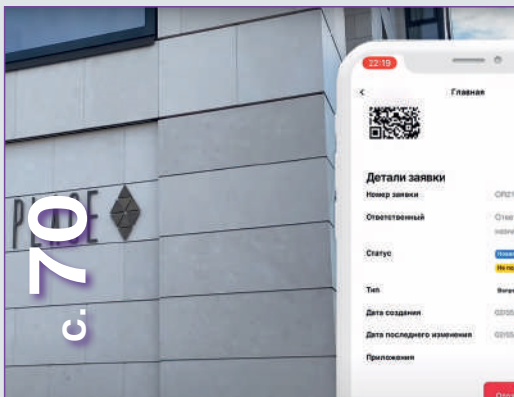
14
с



И. Бакланов.
О дивный старый мир!



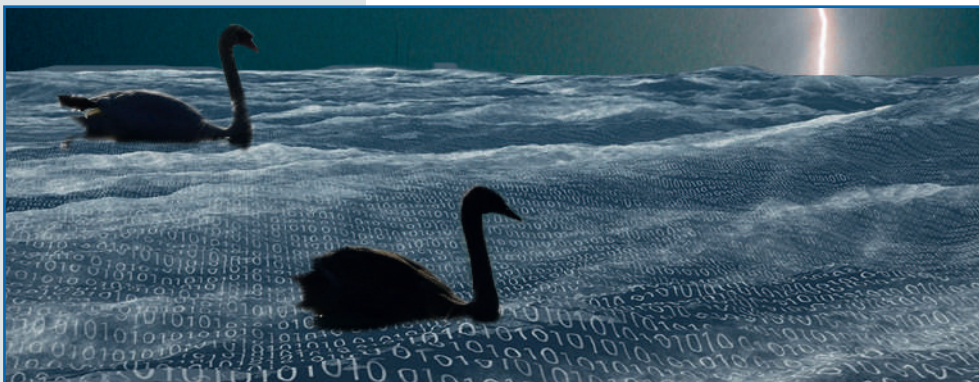
Д. Бизо, Л. Саймон, Ж. Дэвис.
Прямое жидкостное охлаждение: переход неизбежен



Н. Носов. Многоквартирное жилье становится умнее

Н. Носов. Шпаргалки для киберкомиссаров

с. 74



- 32** Г. Юдин, А. Кузнецова. Выбор оптимальной концепции охлаждения майнингового ЦОДа
- 35** Д. Бизо, Л. Саймон, Ж. Дэвис. Прямое жидкостное охлаждение: переход неизбежен
- 42** А. Соловьев. Трансформация бизнеса, трансформация продуктового предложения
- 44** А. Семенов. Архитектура Spine – Leaf в ЦОДах: зачем нужна и как реализовать
- 47** Н. Куликов. Wi-Fi на 6 ГГц. Куда все идет?
- 50** А. Яковлев. «Мы ориентируемся на стандарты качества мировых лидеров СКС»
- 52** Н. Носов. Удаленный доступ через VPN в новой реальности
- 56** А. Зуев. EMILINK: собственное производство = оптимальная цена + контроль качества

58 Сервисы и приложения

- 58** Н. Носов. ЦОДы и облака: трудности и надежды
- 62** О. Роджерс. Основные принципы масштабируемости и устойчивости облаков
- 70** Н. Носов. Многоквартирное жилье становится умнее

74 Безопасность

- 74** Н. Носов. Шпаргалки для киберкомиссаров
- 77** Н. Носов. Остановить телефонных мошенников

79 Новые продукты

Рынок ЦОДов: рост на фоне спада

Несмотря на сложную экономическую ситуацию, рынок ЦОДов продолжает расти. Делегаты 17-го международного форума «ЦОД», организованного в Москве «ИКС-Медиа», смотрят в будущее с оптимизмом.

Ситуация на рынке ЦОДов после начала СВО на Украине сильно изменилась, что повлияло и на главную российскую конференцию в области дата-центров, которую в этом году посетили более 900 делегатов, а еще свыше 550 присутствовали онлайн. Если в прошлом году около половины спонсоров московской конференции «ЦОД» составляли зарубежные вендоры, в основном – западные, то теперь доля иностранных компаний сократилась до 10%, причем преобладали среди них китайские поставщики.

Россия стала мировым лидером по наложенным санкциям, что не могло не сказаться на экономике. По прогнозам Минэкономразвития, падение ВВП в 2022 г. составит 4,2%, спад производства продолжится в 2023 г. – ВВП снизится на 2,7%. Сократились возможности привлечения иностранного капитала, возникли проблемы с оплатой, нарушилась логистика поставок оборудования, увеличились сроки окупаемости инвестиций.

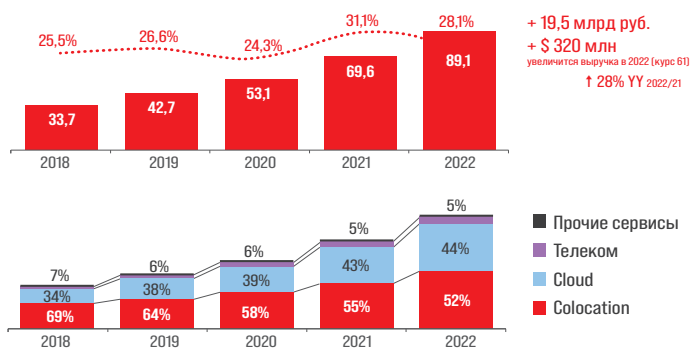
Трудно прогнозировать дальнейшее развитие геополитической ситуации, новые санкции и ограничения. «Неопределенность повышает спрос на услуги аутсорсинга», – отметил ведущий консультант iKS-Consulting Станислав Мирин. По предварительным оценкам аналитического агентства, темпы роста рынка ЦОДов в те-

кущем году (28,1%), хотя и снизились по сравнению с рекордными показателями прошлого года (31,1%, рис. 1), остаются внушительными, особенно на фоне спада во многих отраслях экономики и ухода ряда зарубежных компаний.

Наибольшую востребованность показали облачные услуги. Так, по прогнозам iKS-Consulting, в этом году рынок IaaS вырастет на 40,7% и достигнет 75,7 млрд руб. (рис. 2).

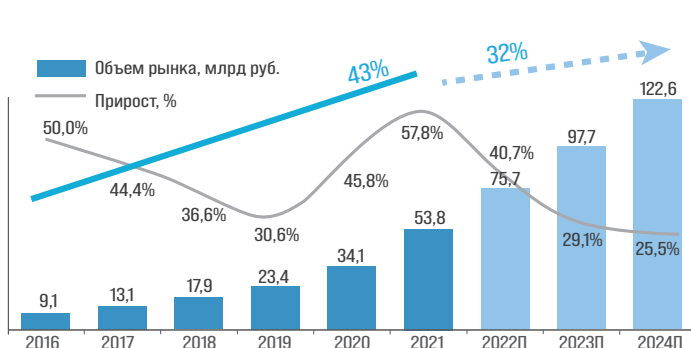
За счет роста облачных сервисов доля услуг colocation в общей выручке коммерческих ЦОДов снижается. Причем часть дата-центров, ранее предоставлявших только услуги colocation, перешла к гибридной модели (и colocation, и cloud), а использующие гибридную сконцентрировались на облачных услугах (рис. 3).

Некоторые дата-центры идут еще дальше и выходят на рынок системной интеграции, помогая миграции ИТ-инфраструктуры заказчиков и оптимизации используемых ими решений. «Переезд – это не перевозка “железа”, а аудит информационных систем», – считает директор по ИТ компании Охуген Александр Будкин. Компания помогает заказчикам и готовит проекты миграции с учетом сетевой связности и особенностей технического решения.



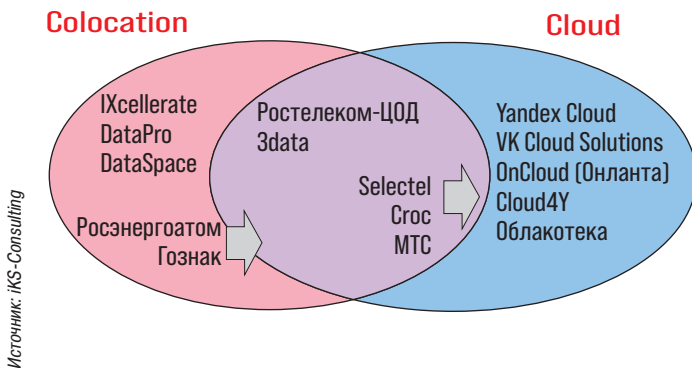
Источник: iKS-Consulting, предварительные данные

▲ Рис. 1. Объем рынка ЦОДов в РФ, млрд руб.



Источник: iKS-Consulting

▲ Рис. 2. Динамика роста рынка IaaS в России



Источник: ИКС-Consulting

Рис. 3. Типы игроков рынка коммерческих ЦОДов и облаков

Свято место пусто не бывает

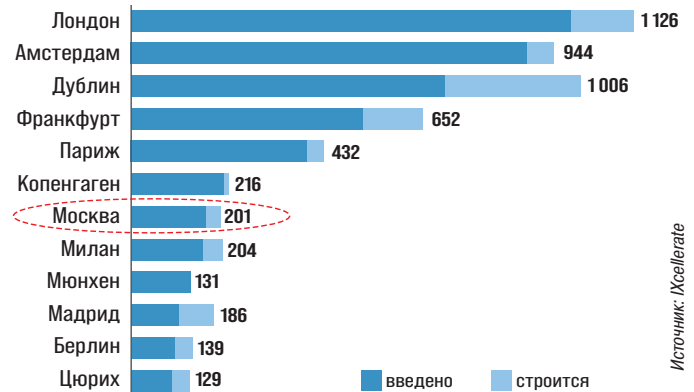
Практика занесения нашей страны в «черные» списки докатилась и до рейтинга рынков ЦОДов Европы, из которого исключили Россию. Компания IXcellerate в представленных на конференции данных исправила ситуацию, и стало видно, что Москва занимает неплохую седьмую позицию (рис. 4) и даже, как считает генеральный директор IXcellerate Андрей Аксенов, может побороться за попадание в первую пятерку.

Рост российского рынка ЦОДов уходом западных компаний замедлить не сможет. Хотя в текущем году зарубежные клиенты, по данным IXcellerate, уже сократили размещение своих стоек (или рассматривают эту меру) в дата-центрах Москвы на 750–1000 единиц, что составляет 2–2,5% рынка Москвы или 1,5–2% рынка РФ, большую часть высвобождающихся стойко-мест занимают отечественные компании, т.е. происходит перераспределение долей рынка между российскими и иностранными клиентами.

Да и западные компании не могут уйти совсем – в России остаются уже построенные и работающие заводы, обладающие высокой квалификацией кадров. Ставший уже типичным путь ухода – продажа бизнеса локальному руководству. Именно так поступила компания Schneider Electric. В результате появилась российская компания Systeme Electric, которой перешли российские активы французского гиганта: заводы «Потенциал» (г. Козьмодемьянск), «ЭлектроМоноблок» (СЭЗЭМ, г. Коммунар), НТЦ «Механотроника» (Санкт-Петербург), Центр инноваций (Иннополис) и крупный инженерно-сервисный центр в Москве, имеющий филиалы по всей России. «У нас есть официальная авторизация на оказание сервисных услуг по всему спектру продукции Schneider Electric. Мы являемся единственным авторизованным партнером с доступом к технологиям, запасным частям и обучению по всему спектру оборудования Schneider Electric», – пояснил первый заместитель генерального директора по рынку «ИТ-решения и сервисы» Systeme Electric Роман Шмаков.

Внимание к регионам

Зарубежные компании проявляли интерес к дата-центрам только в столице, где сконцентрирован основной



Источник: IXcellerate

Рис. 4. Мощности основных рынков ЦОДов Европы на 31.12.2021, МВт

платежеспособный спрос. Развитием ЦОДов в регионах и раньше занимались только российские компании. «Если в Москве наблюдается дефицит стоек, то в регионах предложение отсутствует вовсе. А федеральные компании на региональных рынках нуждаются в том же уровне сервиса и надежности инфраструктуры, которая есть в Москве», – отметил генеральный директор «Кей Поинт Групп» Александр Мартынюк. Он перечислил трудности работы на региональных рынках: не сформировавшийся в явном виде спрос на услуги ЦОДов, проблемы удаленного управления бюджетом и качеством проектов, почти полное отсутствие профессиональных операторов ЦОДов и кадровые сложности на этапе эксплуатации.

Но все это не останавливает российских игроков. Совместно с компанией «Свободные Технологии Инжиниринг» группа реализует мегапроект строительства региональных ЦОДов. «На Дальнем Востоке планируется построить восемь объектов, в Сибири и на Юге – по шесть, на Урале, в Поволжье, на Северо-Западе без Санкт-Петербурга – по пять», – поделился планами генеральный директор «Свободные Технологии Инжиниринг» Евгений Виццер. Причем все объекты будут соответствовать уровню надежности Tier III. Среди крупных клиентов – «Вымпелком», который отошел от традиционного для телеком-гигантов подхода строительства собственных ЦОДов.

По модели франшизы движется в регионы компания 3data. В 2020 г. она запустила дата-центр в Омске. В 2021 г. в партнерстве с «Кей Поинт Групп» началось строительство дата-центра во Владивостоке. «В ближайшие месяцы площадка примет первых клиентов», – сообщил генеральный директор 3data Илья Хала. Идет выбор площадки под ЦОД в Иркутске. В 2022 г. в партнерстве с Alias Group стартовал проект в Краснодаре – ввод объекта в эксплуатацию намечен на следующий год.

Время возможностей

С уходом зарубежных вендоров у российских компаний появились новые возможности для роста. Ведь никуда не исчез главный движущий фактор развития отрасли – активно продолжающаяся цифровизация, которая подразумевает переход на цифровые сервисы и



На панельной дискуссии

стремительное увеличение объема накапливаемых и обрабатываемых данных.

Из-за невозможности поставок российских товаров в Европу серьезные изменения затронули и зарубежные предприятия российских фирм. Например, компания ДКС, монополист (93%) на рынке кабеленесущих систем в Италии, поменяла концепцию работы. «Если раньше наши заводы зависели друг от друга, то теперь мы приняли решение, что каждый рынок имеет полноценные локальные заводы со всей линейкой продуктов. И российские заводы работают только на рынок России и СНГ», – пояснил руководитель отдела продаж ИТ компании ДКС Денис Горяченков. До конца года ДКС полностью локализует в России производство шинопроводов и перестанет зависеть от скачков цен на алюминий в Европе.

При этом компания не пытается вытеснить с рынка российских конкурентов, а замещает продукты ушедших вендоров и развивает новые направления, в частности, солнечную энергетику, и уже поставляет зарядные станции для электромобилей.

Нормативный драйвер

Ситуация на российском рынке ЦОДов в целом благоприятная, но это не значит, что рынку не нужна поддержка государства. «Нормативное обеспечение – тоже драйвер развития отрасли ЦОДов», – подчеркнул дирек-



Дискуссии на стендах выставки

тор департамента цифровой экономики «РТК-ЦОД» Дмитрий Панышев.

Правила игры государство вырабатывает в диалоге с бизнесом. В 2019 г. вышли два основополагающих документа: Концепция создания государственной единой облачной платформы и постановление правительства «О проведении эксперимента по переводу информационных систем и информационных ресурсов федеральных органов исполнительной власти и государственных внебюджетных фондов в государственную единую облачную платформу...», которые стали основой для деятельности межведомственной рабочей группы (МРЦ), созданной Минцифры в марте 2021 г.

Благодаря активной работе МРЦ и АНО «Координационный совет по ЦОДам и облачным технологиям», объединившей ведущие компании рынка, были сформулированы поправки в закон «О связи», которыми вводится определение ЦОДа как сооружения связи, дается определение оператора ЦОДа и ставится задача разработки классификации дата-центров. В апреле поправки прошли первое чтение в Государственной Думе, и ожидается, что осенью 2022 г. они будут приняты.

Вторая группа важных поправок подготовлена в Федеральный закон «Об информации, информационных технологиях и о защите информации». Предлагается определить понятия «облачная услуга» и «государственная единая облачная платформа», а также установить требования к платформе и правила ее функционирования. Законопроект прошел треть пути обсуждения и уже согласован с ФОИВ. Окончательное принятие ожидается в 2023 г.

С принятием определения ЦОДа как сооружения связи участники отрасли связывают надежды на более доступную электроэнергию – основную статью расходов дата-центров. Другой важный вопрос, поднятый бизнесом, – необходимость льготного кредитования инвестиционных проектов.

В целом участники конференции, представлявшие основных игроков российского рынка ЦОДов, демонстрировали оптимизм. Да, время трудное, сложностей много, но задачи решаемые, и рынок продолжит расти.

Николай Носов



ГОТОВЫ К РЫВКУ

Во многих странах Центральной Азии и Закавказья созрели предпосылки для стремительного развития индустрии ЦОДов. Таков вывод прошедшего в начале октября в Ташкенте Евразийского форума Data Center & Cloud.

Мероприятие, организатором которого выступила «ИКС-Медиа», а стратегическим партнером – компания Huawei, собрало более 300 делегатов из стран Центральной Азии и Закавказья. Форум стал площадкой для обмена опытом в области проектирования, построения и эксплуатации центров обработки данных. Бурно обсуждались вопросы перевода ИТ-систем и ресурсов компаний и организаций из собственных серверных в профессиональные коммерческие ЦОДы, которые начинают появляться в регионе.

В последние пару лет пандемия придала дополнительный импульс росту и без того динамично развивающегося рынка ИТ-услуг. Однако в странах Центральной Азии и Закавказья объем таких услуг пока невелик. Лидируют по этому показателю, согласно данным iKS-Consulting, Казахстан (\$1687 млн), Узбекистан (\$580 млн) и Азербайджан (\$251 млн). Следом идут Армения (\$50 млн), Грузия (\$30 млн) и Кыргызстан (\$30 млн).

Скромные достижения рынка ИТ-услуг напрямую связаны с небольшим числом коммерческих ЦОДов, которые являются основой их предоставления. Так, в Казахстане насчитывается порядка 2,5 тыс. коммерческих стойко-мест, а в Узбекистане до недавнего времени этот показатель находился на уровне чуть более сотни стоек (здесь и далее данные iKS-Consulting). Для сравнения: в РФ эксплуатируются 52,6 тыс. стойко-мест. Емкость самой крупной площадки в Казахстане – 200 стоек, а в Узбекистане – 50 стоек.

Невелик и объем рынка облачных сервисов: в Казахстане он составляет \$30 млн, в Узбекистане – \$10 млн (для сравнения в РФ – \$820 млн). Уровень проникновения этих сервисов – приблизительно 10 и 1% соответственно.

Татьяна Толмачева, партнер iKS-Consulting, выделяет несколько факторов, сдерживающих развитие рынка ЦОДов и облачного провайдера в Евразии. Во-первых, это низкий уровень конкуренции: в том же Узбекистане всего примерно пять облачных провайдеров. Во-вторых, это монополия государственных операторов связи. Для того чтобы ЦОД стал действительно отказоустойчивой и эффективной площадкой для предоставления ИТ-услуг, он должен быть подключен к независимым каналам связи, предоставляемым разными провайдерами.

Еще одним сдерживающим фактором эксперт считает низкий уровень использования публичной инфраструктуры государством. Здесь стоит заметить, что, если в России доля коммерческих ЦОДов с государственным участием составляет 30%, то в Узбекистане и Казахстане этот показатель гораздо выше: 65 и 80% соответственно.

Наконец, небольшой объем спроса на услуги коммерческих ЦОДов и облачных провайдеров во многом объясняется низкой мотивацией перехода на аутсорсинг.

По оценке, которую приводит Т. Толмачева, в Казахстане 2/3 компаний предпочитают модель in-source, т.е. развивают ИТ-системы на основе собственной инфраструктуры. В Узбекистане же по этой модели работает большинство компаний.



Источник: president.uz



Источник: president.uz

▲ Единый центр хранения и обработки данных «Электронное правительство» (Зангиатинский район, Ташкентская область)

Эксперт прогнозирует, что спрос на услуги коммерческих ЦОДов в Узбекистане будет находиться в ближайшие годы на уровне 100 новых стоек в год. Однако эта оценка, основанная во многом на текущем уровне предложения таких услуг, может быть существенно повышена, если учесть новые проекты, реализация которых уже началась.

ЦОД для госуслуг

Недавно в Зангиатинском районе Ташкентской области в рамках стратегии «Цифровой Узбекистан – 2030» при участии компании Huawei был построен единый центр хранения и обработки данных «Электронное правительство». ЦОД рассчитан на размещение 300 ИТ-стоек, общая электрическая мощность объекта – 5 МВт. В нем установлены 580 серверов и система хранения данных емкостью 20 Пбайт. ЦОД полностью оснащен всем необходимым оборудованием для обеспечения бесперебойного (ИБП) и гарантированного (дизель-генераторы) электропитания и охлаждения ИТ-нагрузки, противопожарными системами и пр. Проект ЦОДа имеет сертификат Tier III, выданный Uptime Institute.

В результате ввода дата-центра в эксплуатацию будут сэкономлены многомиллиардные средства госорганов на хранение данных и техническую поддержку, а также повысится качество услуг, предоставляемых гражданам и предпринимателям. Важно и то, что будет обеспечена надежная защита государственных информационных систем от кибератак.

ЦОД для colocation

Настоящим прорывом для рынка ЦОДов Узбекистана, да и всей Центральной Азии, может стать реализация проекта компании DSS. Как рассказал Эндрю Хардисти, технический директор DSS, компания планирует в г. Нурафшане (Ташкентская область) на участке площадью 12 га построить современный ЦОД Tier III для предоставления услуг colocation общей емкостью 1920 стоек. Этот

проект обещает стать крупнейшим не только в Узбекистане, но и во всем регионе.

Проект рассчитан на две очереди, каждая из которых предполагает возведение комплекса на 960 стоек. В обоих комплексах будет по шесть машзалов, вмещающих 160 стоек. Инфраструктура проекта рассчитана на то, что средняя мощность потребления одной стойки составит 6 кВт, но в проект закладывается и возможность установки стоек с более высокой мощностью.

Система гарантированного и бесперебойного электропитания будет построена по схеме резервирования 2N с двумя лучами распределения питания до стоек. Время работы системы гарантированного электропитания при 100%-ной нагрузке на собственных запасах топлива составит не менее 48 ч. Расчетный коэффициент энергоэффективности (PUE) – менее 1,45, что значительно лучше среднего для индустрии показателя 1,57.

На базе нового ЦОДа компания DSS предполагает предоставлять места для размещения клиентских стоек с оборудованием, стойки для размещения оборудования клиентов, а также выделенные зоны и целые серверные залы. DSS планирует получить сертификаты Uptime Institute Tier III всех трех типов: на дизайн (Tier Certified Design), объект (Tier Certified Constructed Facility) и операционную устойчивость (Operational Sustainability).

Перспективы для вендоров

Активизировавшееся строительство цифровой инфраструктуры в регионе, безусловно, привлекает поставщиков соответствующих технических решений. Сразу три крупных международных вендора комплексных решений для инженерной инфраструктуры ЦОДов представили свои продукты на форуме Data Center & Cloud – Huawei, Schneider Electric и Delta Electronics. Продуктовые портфели этих компаний включают в себя все основные компоненты инженерной инфраструктуры, в том числе ИБП, системы охлаждения, шкафы/стойки для



Источник: DSS

▲ Макет будущего ЦОДа компании DSS в г. Нурафшане (Ташкентская область)

размещения ИТ-оборудования, а также системы управления инженерными комплексами дата-центров.

Компания Siemon представила делегатам форума свои кабельные системы для ЦОДов, Sabero – системы охлаждения, а H3C, xFusion, как и упомянутая Huawei, – решения для ИТ-инфраструктуры. Интерес вызвал новый для Центральной Азии подход к построению ЦОДов на основе быстровозводимых конструкций, с которым познакомил слушателей компания Jet Infosystems Central Asia. В России этот подход уже успешно используется, в частности, компаниями «Свободные Технологии Инжиниринг» и «Ди Си квадрат» при создании ЦОДов Key Point. Он позволяет существенно сократить сроки строительства при обеспечении высокого качества.

Перспективы рынка цодостроения Центральной Азии привлекли в Ташкент и российских производителей – несмотря на резкий рост количества заказов в России. Свои продукты представили компании Systeme Electric (обра-

зована в результате продажи бизнеса Schneider Electric в РФ и Беларуси локальному руководству), C3 Solutions и Emilink, которые также претендуют на роль поставщиков полного спектра решений для инженерной инфраструктуры ЦОДов.

Время для прорыва

Для прорывного развития евразийского рынка дата-центров и облачного провайдера нужны, по мнению Т. Толмачевой, три критических условия:

- благоприятные условия для частных инвестиций в цифровую инфраструктуру;
- внутренний спрос на услуги хранения и обработки данных;
- обеспечение равного доступа игроков рынка к инфраструктуре связности.

И, как показал Евразийский форум Data Center & Cloud, по крайней мере в Узбекистане эти условия уже складываются. В частности, компании с интересом относятся к возможности использовать услуги colocation, что позволит им избавиться от необходимости строить, укомплектовывать персоналом собственные серверные комнаты или центры обработки данных и управлять ими, сконцентрировавшись вместо этого на ключевых задачах бизнеса. Дело за малым: строить коммерческие ЦОДы, способные такие услуги предоставлять.

В целом ташкентский форум позволяет предположить, что индустрия ЦОДов наиболее активно проводящих цифровизацию стран Центральной Азии и Закавказья находится на пороге бурного роста. Наличие надежных дата-центров в каждой из стран Евразийского региона будет способствовать развитию цифровой экономики, единого цифрового пространства, трансграничных цифровых инфраструктур и экосистем.

Александр Барсков
Ташкент – Москва



Казахстан задает цифровую моду



Стремительное развитие рынка ЦОДов и облачных сервисов в Республике Казахстан во многом стимулировано государственными программами.

Как показал организованный «ИКС-Медиа» в Алматы форум Data Center & Cloud Kazakhstan, рынок коммерческих дата-центров и облачных сервисов Казахстана находится в стадии бурного роста. По данным, которые привела Светлана Черненко, глава представительства iKS-Consulting в Казахстане, за три года – с 2019-го по 2022-й – количество стойко-мест в коммерческих ЦОДах удвоилось и достигло почти 2,5 тыс. (рис. 1).

Рост доходов коммерческих ЦОДов также впечатляет: за указанный период – с 9,1 до 17,9 млрд тенге. По прогнозу iKS-Consulting, к 2025 г. этот рынок увеличится до 25,8 млрд тенге.

И это, по-видимому, только начало. Согласно оценке Сырыма Толеулиева, заместителя председателя правления «Казтелепорта», сегодня более 80% компаний продолжают использовать для информационных систем собственные серверные. По мере повышения популяр-

ности ИТ-аутсорсинга коммерческие ЦОДы будут укрупняться и их будет становиться больше.

Серьезным стимулом развития отрасли ЦОДов в Казахстане С. Черненко считает полномасштабную цифровизацию всех отраслей экономики страны, осуществляемую в рамках государственной программы «Цифровой Казахстан» и проектов DigitEl, SmartCity, eHealth и др. Стремительно растет объем оцифрованных данных и, как следствие, повышается спрос на их хранение. Набирают темпы локализация зарубежных (глобальных) и развитие местных облачных сервисов. Наконец, владельцы дата-центров и сервис-провайдеры все активнее выстраивают взаимовыгодные партнерские отношения.

Главные проекты

Наиболее значимый вклад в развитие казахстанского рынка ЦОДов в 2020–2022 гг. внесли проекты, реализованные компаниями «Транстелеком», QazCloud, «Казахтелеком» и «Казтелепорт».

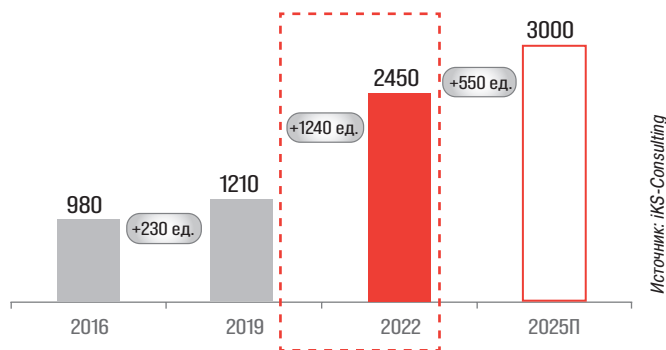
Так, «Казахтелеком» в 2021 г. запустил модульный дата-центр в Алматы, рассчитанный на 168 стоек (с акцентом на виртуализацию ИТ-мощностей) и соответствующий уровню Tier II. Компания QazCloud, созданная в первую очередь для предоставления услуг государственным органам, построила ЦОД на 100 стоек в посел-



С. Черненко



С. Толеулиев



▲ Рис. 1. Рост количества стоек в коммерческих ЦОДах Казахстана

ке Косшы рядом с Астаной. Этот объект также соответствует требованиям Tier II.

«Транстелеком» в 2020–2021 гг. ввел в эксплуатацию сеть ЦОДов в семи городах страны (рис. 2). Сеть состоит из соответствующих требованиям Tier III типовых объектов по 96 стоек в каждом с возможностью расширения. Сейчас у компании десять ЦОДов в девяти городах (Актау, Алматы, Актобе, Астана, Атырау, Жезказган, Караганда, Кызылорда и Уральск) общей емкостью более 800 стоек. Благодаря новым ЦОДам, размещенным в непосредственной близости к конечным заказчикам, компании удалось устранить существовавший в Казахстане региональный дисбаланс, когда ЦОДы располагались преимущественно в Алматы и Астане.

«Казтелепорт», располагающий сетью из семи ЦОДов (в Алматы, Астане и Актау, рис. 3), в 2022 г. запустил новый ЦОД «Сайрам» в Алматы. Объект рассчитан на 120 стоек (мощность каждой до 6 кВт) и примечателен тем, что это первый коммерческий ЦОД в Казахстане, который получил сертификат Tier III Facility от Uptime Institute. В системе бесперебойного электропитания ЦОДа «Сайрам» применяются литий-ионные батареи, способные обеспечивать его работоспособность до 20 мин, а расчетный коэффициент энергоэффективности (PUE) не превышает 1,2.

Связанные одной цепью

Инфраструктурный прорыв позволяет активно развивать цифровые сервисы, в первую очередь по облачной модели. По данным iKS-Consulting, совокупный объем рынка облачных услуг с учетом прямых государственных закупок в 2021 г. превысил 16,22 млрд тенге. При этом государство и квазигосударственные компании обеспечивают более половины всего объема заказов этих услуг. Формируемая государством мода на облака подтягивает «в цифру» бизнес и общество.

Три четверти объема облачного рынка в стране приходится на инфраструктурные услуги (IaaS, рис. 4). В оставшейся четверти доминирует SaaS. В этом сегменте в основном присутствуют локализованные версии зарубежных продуктов и используются агентские модели продаж. Невысокое потребление услуг PaaS аналитики связывают с незначительным объемом местных разработок. Но в целом структура запросов на облачные сер-

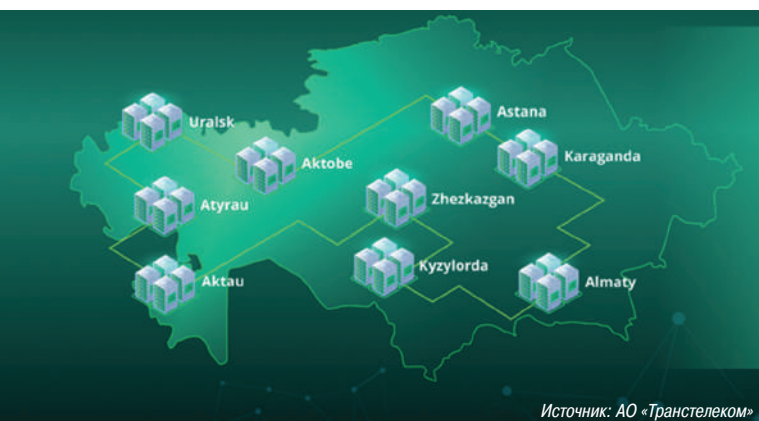


Е. Минавар

висы усложняется. Растет спрос на услуги безопасности, резервного копирования и хранения данных.

Три важных события в 2021–2022 гг. на облачном рынке Казахстана произошли с участием российских провайдеров. Так, в 2021 г. «Яндекс» вывел на рынок платформу Yandex Cloud с акцентом на локализацию сервисов на базе машинного обучения и аналитики больших данных, а также инструментов для разработчиков. Другой крупный игрок – компания VK – также в 2021 г. заключила соглашение с QazCloud о запуске облачной платформы VK Cloud Solutions на базе инфраструктуры ЦОДов QazCloud. Анонсирован доступ для казахстанских предприятий к широкому спектру решений для управления бизнес-процессами. Наконец, уже в 2022 г. меморандум о сотрудничестве и совместном предоставлении облачных решений подписали «Казакхтелеком» и «ИТ Град». Предполагается ориентация на сегменты B2B и B2O.

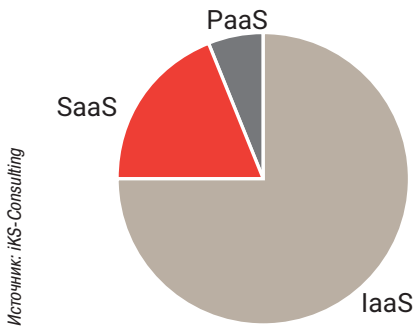
Многие эксперты говорят о том, что в Казахстане пришло время локализации облачных сервисов. Ерлан Минавар, заместитель председателя правления «Транстелекома» по стратегическому развитию и инновациям, выделяет три основные предпосылки для такой локализации. Во-первых, необходимость защиты данных: в республике действует закон о защите персональных данных, согласно которому данные граждан не должны размещаться за границей. Во-вторых, необходимость сни-



▲ Рис. 2. Сеть ЦОДов АО «Транстелеком»



▲ Рис. 3. Сеть ЦОДов АО «Казтелепорт»



▲ Рис. 4. Структура рынка облачных сервисов Казахстана, 2021 г.



▲ Рис. 5. Уровни зрелости разных категорий владельцев/операторов ЦОДов по четырем основным векторам развития отрасли

жения стоимости трафика и уменьшения задержки: «Облачная платформа Google или Microsoft Azure — это хорошо, но нелогично размещать приложения в Стокгольме, когда вся ваша аудитория — местная», — указывает Е. Минавар. И в-третьих, стремление оставлять деньги в стране: доходы от предоставления облачных сервисов используются для развития экономики Казахстана.

«Транстелеком» развивает облачные сервисы на базе сети своих ЦОДов. Среди предлагаемых компанией услуг – виртуальные частные облака, сервисы безопасности, объектные хранилища, кластеры Kubernetes, резервное копирование и т.д. При этом она делает ставку на партнерство со стартапами через корпоративную инновационную программу. Стоит также отметить, что благодаря расположению ЦОДов в непосредственной близости от заказчиков компания в полной мере может реализовать концепцию Edge Cloud, что позволяет обслуживать приложения, которым требуется минимальная задержка. Это важно, в частности, для производственных предприятий.

Активен на облачном рынке и другой владелец крупной сети коммерческих ЦОДов – «Казтелпорт». Помимо классических IaaS (на базе VMware и KVM) и PaaS, компания предлагает сервисы BaaS, DRaaS, Finance Cloud (облако, сертифицированное по стандарту PCI DSS), гибридное облако, а также широкий набор услуг информационной безопасности.

В поиске оптимального решения

Любая конференция – это всегда обмен наилучшими практиками и поиск оптимальных решений. Не стала исключением и Data Center & Cloud Kazakhstan. Александр Мартынюк, исполнительный директор компании «Ди Си квадрат», поделился своим опытом использования модульного подхода, и не только к построению отдельных объектов, но и к развитию рынка ЦОДов в целом. Среди плюсов такого подхода – возможность постепенного наращивания мощностей ЦОДов, распределение капитальных затрат во времени, типизация строительства и снижение стоимости эксплуатации. Кроме того, А. Мартынюк выделил повышение общей экономической привлекательности проекта и гибкость в его адаптации к потребностям клиентов.

«Отрабатывать решения на небольших модулях безопаснее и проще, — подчеркнул он. — А повторяемость решений существенно облегчает жизнь службе эксплуатации. Мо-

дульность снижает риски, повышает экономическую привлекательность проекта и упрощает его развитие». Следует отметить, что модульный подход применяется в реализации сети региональных ЦОДов Key Point в России. В зависимости от потребностей конкретного региона Key Point предлагает решения разных масштабов: XL (400–1200 стоек), L (200–400 стоек), M (50–200 стоек) и S (30–100 стоек).

Денис Вайнер, директор по продажам в странах СНГ компании Schneider Electric, заявил, что сегодня заказчиков по большому счету не интересует, как устроена инфраструктура, их интересует доступность сервисов. Для ее повышения он рекомендует использовать гибридную иерархическую архитектуру сети ЦОДов. Нижний уровень такой архитектуры представляют периферийные (edge) узлы, которые, как правило, основаны на стандартизованных и унифицированных элементах. Следующий уровень – региональные ЦОДы; они строятся на уже адаптированных решениях. Наконец, верхний уровень – головной ЦОД, который базируется на уникальной архитектуре.

Эксперт Schneider Electric считает, что будущее ЦОДов будут определять четыре вектора: устойчивое развитие, повышение эффективности, адаптивности и надежности (рис. 5). На данный момент строители ЦОДов думают прежде всего об эффективности и надежности. Но все больше компаний начинают обращать внимание на устойчивое развитие, которое предполагает выработку углеродной стратегии, оптимизацию управления ресурсами, применение возобновляемых источников энергии и перерабатываемых материалов, включая аккумуляторные батареи. Важна и адаптивность: гибкость в проектировании, развертывании и обслуживании, совместимость с ИТ-системами следующего поколения, внедрение программно определяемых систем и активное управление энергией.

Сегодня ЦОДы становятся не только критически важной ИТ-инфраструктурой отдельных предприятий, но и стратегическим активом государств. Казахстан задал высокий уровень цифрового развития. И результаты налицо. Так, в недавно опубликованном рейтинге ООН, отражающем электронное участие граждан во взаимодействии с государством (E-Participation Index), страна заняла высокое 15-е место. И индустрия ЦОДов и облачных сервисов готова этот уровень не только поддерживать, но и повышать.

Александр Барсков
Алматы – Москва



НОВОСТИ ОТРАСЛИ

В России появился новый индекс цен на услуги colocation

iKS-Consulting и 3data анонсировали результаты ежеквартального ценового исследования и первый в России индекс цен на услуги colocation в агломерациях «Москва» и «Санкт-Петербург». Как показало исследование iKS-Consulting, проведенное в августе-сентябре 2022 г., средняя цена на услуги colocation – аренду места для размещения ИТ-оборудования в ЦОДе – в агломерациях «Москва» (включает Москву и ближайшее Подмосковье) и «Санкт-Петербург» (включает Санкт-Петербург и Ленинградскую область) составила 109,6 и 69,5 тыс. руб. без НДС соответственно. Таким образом, в сентябре 2022 г. индекс цен на услуги colocation – 3DCI (3data Colocation Index) – в сравнении с показателем за II квартал (апрель 2022 г.) в Московском регионе составил 107,6%, в Санкт-Петербурге – 102,6%.

ЦОД Tier III в Узбекистане

В рамках стратегии «Цифровой Узбекистан – 2030» создан центр хранения и обработки данных высокой производительности. ЦОД рассчитан на размещение 300 ИТ-стоек, общая электрическая мощность объекта – 5 МВт. ЦОД полностью оснащен всем оборудованием, необходимым для обеспечения бесперебойного (ИБП) и гарантированного (дизель-генераторы) электропитания и охлаждения ИТ-нагрузки, противопожарными системами и пр. Проект имеет сертификат Tier III, выданный Uptime Institute.

«Ростелеком» открыл свой первый ЦОД в арктической зоне России

«Ростелеком» ввел в промышленную эксплуатацию ЦОД в Мурманске. Якорным заказчиком проекта выступило правительство Мурманской области. Клиенты дата-центра станут как органы власти региона, так и представители бизнеса. Емкость регионального ЦОДа составляет 20 стоек. При увеличении потребностей проектом предусмотрено быстрое наращивание мощностей.

МТС построила модульный ЦОД в Новосибирске

Это первый модульный ЦОД МТС за Уралом и 13-й в федеральной сети дата-центров оператора. Модули удалось развернуть за восемь месяцев, что в несколько раз быстрее, чем строить классический дата-центр. В настоящее время запущены два модуля по 125 стоек полезной мощностью 1800 кВт. Этого достаточно, чтобы обеспечить бесперебойную работу ИТ-инфраструктуры МТС: биллинга, системы онлайн-обслуживания абонентов, оборудования для сетей 3G/4G/5G и других технологий. В течение года МТС планирует увеличить мощности дата-центра в два раза и использовать их для развития облачных продуктов компании. Новый ЦОД имеет сертификат Tier III.

Key Point начинает региональную экспансию



В ходе ВЭФ-2022 Key Point заключила ряд важных соглашений. Так, соглашение с «МегаФон» предусматривает организацию выделенных технологических площадок в дата-центрах Key Point, которые появятся в региональных центрах деловой активности в ближайшей перспективе. С «ВымпелКомом» запланировано инициировать строительство в Новосибирске нового дата-центра Key Point. Соглашение о сотрудничестве с «Ростелекомом» предполагает организацию точки присутствия оператора в ЦОДе Key Point, создаваемом на территории опережающего развития «Надеждинская». С Корпорацией развития Дальнего Востока и Арктики были документально зафиксированы достигнутые ранее договоренности относительно начала второй очереди проекта на TOP «Надеждинская» и проработки вариантов строительства аналогичных дата-центров в Амурской, Сахалинской, Мурманской, Архангельской, Магаданской областях, а также на Камчатке, на Чукотке, в Хабаровском крае, в Якутии и Карелии.

IXcellerate открыла третий дата-центр в России



MOS5 – первый действующий объект в Южном кампусе IXcellerate. Он расположен в Москве в районе Бирюлево и занимает 14 га. Новый дата-центр полностью готов к эксплуатации: функционируют 1516 стойко-мест, обеспеченных электроэнергией в объеме 17 МВт по схеме двойного резервирования. Команда IXcellerate приступила к строительству второй очереди MOS5 на 836 стойко-мест, более 75% из них уже зарезервировано. Ввод в эксплуатацию всех пяти очереди дата-центра намечен на 2024 г. Его совокупная емкость составит 4722 стойко-места, а энергоемкость – 64 МВт.

В Твери открыт ЦОД Федеральной таможенной службы



ЦОД станет основной площадкой централизованной обработки данных, поступающих от таможенных органов. Площадь ЦОДа – 3200 кв. м. Общий объем хранения информации – 13 Пбайт. В ЦОДе применено техническое решение, которое позволяет обслуживать любую из его подсистем без остановки работы объекта в целом, что гарантирует бесперебойное оформление товаров по всей стране. Электропитание и каналы связи проведены по разным линиям, имеют независимые трассы и предоставляются разными провайдерами. ЦОД оснащен дизельными генераторами и может автономно работать 12 ч.

«Яндекс» строит в Калуге свой крупнейший ЦОД



ЦОД, который станет новой точкой доступности Yandex Cloud, будет располагаться на территории промышленного парка «Грабцево». Его открытие намечено на второе полугодие 2023 г. В ЦОДе разместятся более 3,8 тыс. серверных стоек с нагрузкой по 15 кВт. Площадь ЦОДа – 130 тыс. кв. м, общая проектная мощность – 63 МВт. Планируемый среднегодовой PUE – 1,07–1,09. Дата-центр будет обеспечивать работу и внутренней инфраструктуры сервисов «Яндекса», и облачной платформы.

Гособлако приземлится в Саратове

Заместитель председателя правительства Дмитрий Чернышенко, посетив строящийся в Балакове (Саратовская область) региональный дата-центр Сбербанка, сообщил, что Минцифры поручено совместно со Сбером проработать вопрос использования вычислительной инфраструктуры регионального центра для геораспределенного резервирования сервисов цифровой платформы «Гостех» и гособлака. Объект соответствует операционной устойчивости уровня Tier III. Планируется, что потребляемая мощность составит 82 МВт, а годовой показатель PUE – 1,1–1,4.



О дивный старый мир!

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

Сегодня, после стольких лет топтания на месте, российские инженеры могут и должны сохранить и развить знания, восстановить суверенитет и самостоятельность мышления нашего общества. Из ступора пора выходить.



Вы, русские, – еще римляне
или уже итальянцы?
Евгений Водолазкин. «Брисбен»

Наше время создает уникальные возможности для дискуссии. На памяти моего поколения это происходит второй раз. Что-то подобное мы испытали в период перестройки конца 80-х, когда на волне гласности стало доступно все скрытое, забытое и даже немислимое. Мы купались в море запрещенных до той поры самиздатских книг, смелых речей, политической полемики, мировоззрений тоталитарных сект, невероятных планов переустройства мира – все казалось возможным и все было по плечу. Это породило оптимизм, граничащий с опьянением идиота. Желание действовать, быть открытым и внести свой вклад в жизнь вело каждого. История шла нам навстречу. В каждой комнате студенческого общежития жил либо поэт, либо философ, либо эзотерик и мистик. Это было время широчайших дискуссий.

Потом наступило отрезвление 90-ми, построение капитализма, осознание того, что описанное Теодором Драйзером и то, о чем говорила советская пропаганда, – оказывается, правда. Мы пытались понять, вписаться, выжить в непривычном и довольно несправедливом мире.

И вот теперь мы снова возвращаемся в пространство дискуссий, хотя и на совершенно другом уровне. У большинства уже нет оптимизма, и мало кто верит, что наши идеи и поступки изменят историю. Советские достижения – от мирного атома, математики, физики до кинематографа, литературы и философии – кажутся чем-то сказочным, наполненным содержанием, творчеством и смыслом, недостижимым и уже частично непонятным. Наше же время – это время осознания происходящего и нового развития. Потому что опасность приходит к нам на порог, и отсидеться не получится. И дело вовсе не в противостоянии СВО, и даже не в противоречиях России и Запада. Дело в том, что мы основательно забыли себя.

В масштабе Человечества

Давайте вернемся в прошлое. Почему К.Э. Циолковский в деревянном скрипучем домике в Калуге рисует чертеж ракеты? Потому что мы – не просто двуногие без перьев, мы – Человечество! Русский космизм говорил о том, что бессмертие – это всего лишь вопрос времени. Рано или поздно мы сами из праха восстановим ушедшие поколения. И тогда нам нужно лететь в космос для того, чтобы расселить воскрешенных, и для того, чтобы собрать прах праотцов, чтобы и их воскресить. Успех толстовской «Аэлиты» и «Собачьего сердца» Булгакова – наглядное отражение того, что было в умах и сердцах.

Люди верили, что в соседнем гараже инженер Лосев вполне может построить космолет, а в соседнем доме профессор Преображенский может из собаки сделать гомункула. Потом эти люди за 10–15 лет создали самую мощную экономику Европы, которая выдержала тяжелейшую в мировой истории войну. А потом за 10 лет после победы они восстановили страну и начали освоение космоса, создали технологию мирного атома, которая почти не изменилась с тех пор, мощнейшую научную школу, совершенную систему среднего и высшего образования.

Сейчас, после стольких лет топтания на месте, хочется понять, как им это удалось? И это не праздное любопытство. Наше поколение должно это понять и использовать, у нас другого выхода нет. Тот подвиг, который совершили деды, мы тоже должны совершить. Или наша участь будет незавидной.

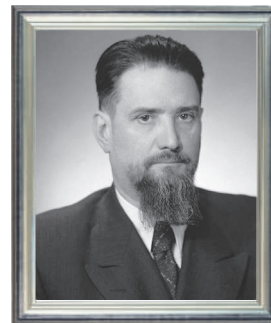
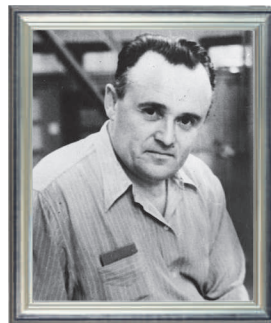
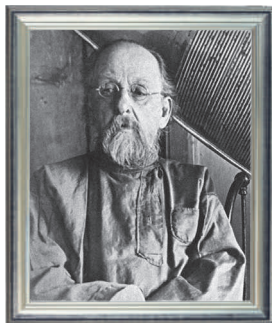
Оборачиваясь на русскую философию и литературу середины 20 века, иногда поражаешься масштабу тех людей. В работах Вернадского, Ефремова, Павлова, Казанцева, ранних Стругацких, Ларионовой ставились вопросы об устройстве будущего, преобразовании Земли и ближайшего космоса, освоении и исследовании подводного мира, Антарктики – все это наследовало традиции широкого шага русского характера, открывающего новые земли, концепции, принципы, законы, гармонию.

Сейчас, на изломе времен, это очень важно помнить. Не только ради славы предков, но и ради жизни потомков.

Мы не построили мир Полудня, мы скатились в мир Часа Быка. Нас встречает Новое Средневековье с комплексом неполноценности потомков, недостойных славы и мощи своих отцов. Вызовы современности требуют осознания, на голых эмоциях с ситуацией не справиться. Со всех сторон нас зовут в «дивный новый мир», пытаются доказать, что альтернативы нет, зомбируют и призывают к одичанию. Под видом торжества гуманитарных наук подсовывают постмодернизм, в котором нет ничего, кроме лжи.

Налево пойдешь – себя потеряешь

Что же остается инженеру в этой ситуации? Все просто – нужно держаться своих корней. Не предавать своего мира и своего призвания, даже если к этому подталкивает вся окружающая среда. Продолжать верить в разум и использовать научно-технические знания в качестве основы для переустройства мира. Помнить, что современная технологическая цивилизация построена инженерами, а не социологами и юристами. И именно инженеры могут и должны восстановить порядок, сохранить и развить знания, восстановить суверенитет и самостоятель-



ность мышления нашего общества. Без революций, без крикливых речей и пышных карнавалов, а каждодневным трудом и ощущением масштаба задач. Учиться этому масштабу у наших предков. Следовать старой одесской половице: «Давайте делать хорошо, плохо само получится». Если мы замахнемся на восстановление культуры, науки всего Человечества, то уж с проблемами страны или своего района точно справимся. Мысли глобально, действуй локально – это во всех учебниках по управлению написано. Так давайте переосмыслим происходящее и начнем что-нибудь делать.

После начала экономической войны нашу отрасль поразил ступор. До «Крымской весны» 2014 г. в среде инженеров было два сообщества: ультралевые и умеренные правые. Ультралевый подход утверждал, что мы отстали на сто, двести, триста лет и потому должны сдаться. Забыть о суверенитете и о самостоятельности мышления. Свести инженерную деятельность к выполнению роли техников, поддерживающих не нами созданные технологии. Весь научно-исследовательский дискурс перевести в область трактовок международных стандартов и размышлений над величию за океанских технологий. Умеренные правые не отрицали потери самостоятельности и технологического суверенитета, но предлагали что-то делать самостоятельно. Хотя бы в нишевых отраслях, хотя бы в каких-то отдельных сегментах. Голос ультраправых был практически не слышен, потому что подавляющее большинство инженерного сообщества оказалось в ультралевом лагере. Первые постперестроечные поколения инженеров были очарованы технологиями Запада, а следующие поколения воспитывались уже в ультралевой доктрине. Достаточно вспомнить «научные» конференции последних лет, где представители IBM и Siemens, русские инженеры, рассказывали о победах в Азии и перспективных проектах в Латинской Америке, произнося через слово многозначное и очень ценное для всей аудитории местоимение «мы». В этом «мы» содержался самый главный наркотик ультралевых – ощущение причастности к мировому научно-

техническому прогрессу. И никто не замечал, что платой за сопричастность оказывался отказ от самостоятельного мышления и любой стратегии, отличной от заокеанских подходов.

После «Крымской весны» стало понятно, что дальнейшее развитие инженерии по ультралевому сценарию становится сложным и опасным. Появились первые санкции и программа импортозамещения. Однако инженерное сообщество не восприняло патриотические призывы всерьез. Отказ от ультралевого подхода носит мировоззренческий характер. Он требует начать мыслить самостоятельно и критически, перестать поклоняться современным идеалам (Илон Маск, Стив Джобс, Билл Гейтс) и вспомнить забытые (Туполев, Королев, Курчатов и пр.). Такая перестройка мировоззрения порождает экзистенциальный кризис, и в 2014 г. для него явно не хватало оснований.

Инженер – это звучит гордо!

Кризис грянул в феврале и продолжается до сих пор. Большая часть инженерного сообщества оказалась в ступоре. Многолетнее идолопоклонство перед Западом и отсутствие самостоятельного мышления на всех уровнях привело к необходимости поклониться Востоку. Поклонились китайцам, но те как-то не приняли русских как братьев. Тогда поклонились Ирану, но и здесь все неоднозначно. Что дальше? ЮАР, Бразилия, Мозамбик? А пока оцепенение, надежды на параллельный импорт – костыли, костыли, костыли... Семь месяцев ожидания непонятно чего. Слепая мистическая вера, что все наладится...

Давайте честно признаем – не наладится. Вернее, прошлое никогда не вернется. Но мы можем с сегодняшнего дня начать строить новое будущее. Возможно, нас ждет выбор между плохим и худшим. Возможно, будет много ошибок. Но из ступора инженерам пора выходить. Нужна новая идеология от инженерии. Нужен кураж, подобный тому, что был в начале 20 века. Лучше верить, что в соседнем гараже инженер Лосев делает космолет, чем в то, что китайцы или иранцы станут нашими единственными партнерами. И да, нужно вспомнить наконец, что такое русский инженер! **ИКС**



Цифровой рубль становится ближе

Банк России ускоряет ввод цифрового рубля – уже в 2023 г. планирует запустить пилотные расчеты, в том числе с использованием смарт-контрактов. В 2024 г. к платформе цифрового рубля начнут поэтапно подключать все российские банки.

Николай Носов

Этапы большого пути

Банк России анонсировал дорожную карту введения в стране третьей формы денег: на своем сайте регулятор опубликовал проект «Основные направления единой государственной денежно-кредитной политики на 2023 г. и период 2024–2025 гг.». В документе он разъясняет свой взгляд на реализацию денежно-кредитной политики в новых экономических условиях – действия санкций и ухода с россий-

ского рынка ряда иностранных игроков, а также дает сценарии развития экономики на ближайшие три года.

Согласно прогнозу Банка России, в декабре 2022 г. годовая инфляция достигнет 12–15% (см. таблицу). Валовый внутренний продукт упадет на 4–6%, в 2023 г. – еще на 1–4% и стабилизируется лишь в 2024-м. Но это не повод отказываться от планов цифровизации, которая поможет справиться с новыми вызовами. В частности, снижение транзакционных издержек при вве-

Прогноз Банка России в рамках базового сценария ▼

	2020 (факт)	2021 (факт)	2022	2023	2024	2025
Основные макроэкономические показатели (прирост в % к предыдущему году, если не указано иное)						
Инфляция, %, декабрь к декабрю предыдущего года	4,9	8,4	12,0–15,0	5,0–7,0	4,0	4,0
Инфляция, в среднем за год, % к предыдущему году	3,4	6,7	13,8–14,7	4,3–7,5	4,1–4,9	4,0
Ключевая ставка, в среднем за год, % годовых	5,1	5,7	10,5–10,8	6,5–8,5	6,0–7,0	5,0–6,0
Валовой внутренний продукт – %, IV квартал к IV кварталу предыдущего года	-2,7 -1,3	4,7 5,0	(-6,0)–(-4,0) (-12,0)–(-8,5)	(-4,0)–(-1,0) 1,0–2,5	1,5–2,5 1,0–2,0	1,5–2,5 1,5–2,5
Расходы на конечное потребление – домашних хозяйств	-4,9 -7,4	7,2 9,5	(-5,0)–(-3,0) (-6,5)–(-4,5)	(-2,5)–(+0,5) (-3,0)–0,0	1,5–2,5 2,0–3,0	1,5–2,5 1,5–2,5
Валовое накопление – основного капитала	-4,1 -4,6	8,9 6,8	(-22,0)–(-18,0) (-7,5)–(-3,5)	9,5–13,5 (-4,5)–(-0,5)	4,5–6,5 1,5–3,5	2,5–4,5 1,5–3,5
Экспорт	-4,1	3,5	(-17,0)–(-13,0)	(-12,5)–(-8,5)	(-1,0)–(+1,0)	0,0–2,0
Импорт	-11,9	16,9	(-31,5)–(-27,5)	(-1,5)–(+2,5)	2,5–4,5	1,0–3,0

Источник: Банк России

дении цифрового рубля поддержит конкурентоспособность российской экономики.

Первые тестовые транзакции с платформой цифрового рубля уже прошли в феврале 2022 г. Клиенты ВТБ и ПСБ зарегистрировались как пользователи платформы, открыли цифровые кошельки, обменяли безналичные рубли со своего банковского счета на цифровые рубли и отправили другим пользователям платформы.

Переход на цифровой рубль будет постепенным. В 2022 г. – тестирование платформы, в 2023 г. – пилотные расчеты между физическими лицами, а также физическими лицами и предприятиями на реальных деньгах.

Кроме того, в 2023 г. ограниченному кругу участников будет предоставлена возможность заключения и исполнения на платформе цифрового рубля смарт-контрактов – сделок, автоматически исполняемых при наступлении заранее определенных сторонами условий. Пришедший из сферы криптовалют функционал позволит оптимизировать бизнес-процессы, минимизировать время и издержки при проведении сделки.

В 2024 г. Банк России начнет поэтапно подключать к платформе цифрового рубля все кредитные организации, увеличит количество доступных вариантов платежей и операций с использованием смарт-контрактов. По мере готовности Федерального казначейства станут возможны платежи цифровыми рублями как в пользу государства, так и от государства в пользу физических лиц и предприя-

тий. Банк России начнет сотрудничать с другими центральными банками, разрабатывающими собственные цифровые валюты, для проведения трансграничных и валютно-обменных операций.

В 2025 г. планируется реализовать офлайн-режим цифрового рубля (рис. 1), осуществить подключение небанковских финансовых посредников, финансовых платформ, биржевой инфраструктуры.

Повышение доверия

Дискуссии о схемах и целесообразности введения третьего вида денег, объединяющего преимущества наличного и безналичного цифрового рубля, идут уже два года. На самый радикальный вариант – исключить из цепочки коммерческие банки – регулятор не пошел. Со своими цифровыми рублями в информационной системе Банка России, состоящей как из компонентов централизованной системы, так и распределенных реестров, клиент будет работать через коммерческие банки. Но цифровые рубли, полученные коммерческим банком от клиента, останутся деньгами клиента. Он сможет получить к ним доступ через разные банки, и эти деньги не пропадут с исчезновением финансовой организации, например, из-за отзыва лицензии. Хранение цифрового рубля в контуре информационной системы Банка России повышает доверие населения к безналичным расчетам, ведь, как и в случае наличных денег, цифровые рубли будут обязательством Банка России.

Рис. 1. Офлайн-операции с цифровым рублем ▼



Для совершения офлайн-операций, помимо онлайн-кошелька, клиенту будет открыт **второй кошелек** в цифровых рублях непосредственно **на мобильном устройстве клиента**

Источник: Банк России

В документе представлены основные схемы проводок при работе с цифровым рублем. Например, при обмене наличных денег на цифровые (рис. 2) клиент вносит наличные в кассу банка. Сумма переводится на цифровой кошелек банка в Банке России, оттуда – на цифровой кошелек клиента.

Другие преимущества цифрового рубля

Цифровой рубль позволит создавать инновационные сервисы на основе смарт-контрактов и повысит доступность финансовых услуг, в том числе на отдаленных и малонаселенных территориях России, благодаря

ного предложения, как и обычные цифровые рубли и наличные деньги, и наравне с ними использоваться в расчетах. Банки смогут зарабатывать на дополнительных сервисах, построенных на цифровом рубле.

Финансовая стабильность

По мнению регулятора, введение цифрового рубля и переток средств с банковских счетов клиентов в цифровые кошельки на платформе Банка России не создают рисков для финансовой стабильности. Плавный переход даст возможность кредитным организациям адаптироваться к изменению структуры их балансов. А Банк России будет компенсиро-

Банк России		Кредитная организация		Клиент	
Актив	Пассив	Актив	Пассив	Актив	Пассив
Наличные деньги в кассе	Выпущенные наличные деньги	Наличные деньги в кассе (+100)	Депозит/счет клиента (безналичные средства)	Наличные деньги (-100)	Привлеченный банковский кредит
Требования к кредитной организации	Корсчет кредитной организации	Корсчет кредитной организации	Обязательства перед Банком России	Цифровой кошелек на платформе цифрового рубля (+100)	
	Цифровой кошелек кредитной организации (-100)	Цифровой кошелек на платформе цифрового рубля (-100)		Депозит/счет клиента в кредитной организации (безналичные средства)	
	Цифровой кошелек клиента (+100)	Предоставленные клиенту кредиты			
Изменение баланса	0	Изменение баланса	0	Изменение баланса	0

 Одним цветом обозначены одинаковые категории активов и пассивов

Источник: Банк России

возможности проведения расчетов без доступа к интернету. Цифровые рубли можно будет восстановить при потере устройства, на котором они хранятся.

Кроме того, глава Банка России Эльвира Набиуллина заявляла, что внутри одного банка переводы цифровых денег должны быть полностью бесплатными, т.е. банки не должны взимать комиссию за эту услугу при переводах цифровых рублей между физлицами.

Цифровой рубль выгоден для государства, так как повышает прозрачность платежей. Также введение цифрового рубля позволит реализовать технологию «окрашивания», т.е. возможность выбирать целевое направление использования – например, виды товаров и услуг, за которые можно расплатиться «окрашенными» цифровыми рублями. В результате повысится эффективность целевых государственных расходов, в том числе в рамках госзакупок и госконтрактов. «Окрашенные» цифровые рубли будут являться таким же компонентом денеж-

вать отток ликвидности из банков с помощью существующих инструментов денежно-кредитной политики.

Представляются незначительными и риски для финансовой стабильности, связанные с перетоком средств из банковских депозитов в цифровые рубли в результате так называемого бегства в качество, которое возникает при сомнениях в устойчивости банковского сектора. Удержать деньги клиентов коммерческим банкам поможет система страхования вкладов и начисляемые по вкладам проценты. Чтобы избежать конкуренции с банковским сектором, Банк России решил не начислять проценты на средства в цифровых кошельках на его платформе. Поэтому массового оттока денег из коммерческих банков не ожидается, и они смогут и дальше осуществлять кредитование российской экономики. Введение цифрового рубля не затронет фундаментальные основы функционирования банковской системы. ИКС

▲ Рис. 2. Пример движения средств при пополнении кошелька клиента за счет наличных денег

ИТ-трансформация бизнеса: выстраиваем процесс правильно

В свете ухода с российского рынка многих зарубежных производителей программных решений компании вынуждены спешно мигрировать на отечественные системы, менять ИТ-инфраструктуру и бизнес-процессы в целом.

Кирилл Чеханков,
руководитель
департамента
ИТ-решений,
Konica Minolta

С какими запросами сейчас сталкиваются интеграторы и на что можно заменить популярное западное ПО?

Кому доверить электронный документооборот?

Системы электронного документооборота (СЭД) – одно из фокусных направлений для нашей компании, и сейчас мы сталкиваемся с несколькими типами запросов заказчиков. Прежде всего, это комплексная замена СЭД. Долгие годы в крупных организациях наиболее популярна была канадская система OpenText. Решение считается одним из топовых даже по магическим квадрантам Gartner. Зачастую им пользовались компании, которые могли себе позволить, скажем, ERP-систему от SAP.

Первые звонки о необходимости найти замену OpenText и другим западным решениям прозвучали еще в 2014 г., но активно интересоваться отечественным софтом заказчики начали только год-два назад.

В марте SAP и OpenText, как и многие другие иностранные разработчики, заявили об уходе с российского рынка. Их клиенты столкнулись с аннулированием контрактов. К примеру, крупные ретейлеры, такие как «Магнит» и X5 Retail Group, пользовавшиеся OpenText, вынуждены теперь искать ему замену. Безусловно, система на внутренних серверах пока работает, но тех-

ническую поддержку вендор больше не оказывает. А поддержка крайне важна с точки зрения получения ответов на вопросы, которые возникают при использовании платформы. И если произойдут какие-либо критические инциденты, помощи от разработчика тоже не будет. Поэтому можно сказать, что система работает до первого серьезного сбоя.

В результате мы видим существенно возросший спрос на миграцию с импортных СЭД на российские аналоги. При этом стоит отметить, что системы электронного документооборота – это всегда несколько модулей, которые помогают вести ключевые процессы компании:

- канцелярское делопроизводство;
- договорные обязательства и согласование документов;
- юридически значимый документооборот;
- кадровый электронный документооборот;
- технический документооборот;
- электронный архив.

И что интересно – заказчики сегодня готовы обсуждать каждый из модулей по отдельности, для того чтобы постепенно двигаться в сторону импортозамещения монолитного западного решения.

К слову, в подавляющем большинстве случаев мы не наблюдаем пока, чтобы компании использовали в рамках одной платформы больше двух таких модулей, что обусловлено зрелостью

их бизнес-процессов. Тем не менее для крупных организаций переход на российскую систему электронного документооборота становится масштабным проектом, поскольку у них все процессы связаны с СЭД. И для внедрения разных модулей могут привлекаться разные подрядчики.

В своей практике мы сталкивались с тем, что электронный архив может быть организован, например, в «1С», а документооборот вестись в Microsoft SharePoint. Если для малого и среднего бизнеса подобные подходы в целом приемлемы, то более крупный столкнется с определенными сложностями и даже проблемами. И тут уже стоит подобрать на замену единую систему, которая будет комплексно решать все задачи.

Сейчас для миграции с OpenText заказчики выбирают импортонезависимые отечественные платформы Tessa, Docsvision, ZPlatform и другие продукты из единого реестра российского ПО, готовые заменить иностранные СЭД.

Важно отметить, что система электронного документооборота часто критична для компаний с точки зрения работы с конфиденциальными документами, которые содержат чувствительные данные. И миграция на российские аналоги требуется в первую очередь для обеспечения информационной безопасности, т.е. импортозамещение здесь не модное веяние, а именно необходимость.

Замена ERP: интеграторы спешат на помощь

Еще одно направление, к которому сейчас приковано внимание заказчиков, – ERP-системы. После ухода с рынка ключевых зарубежных игроков мы видим массовый спрос на технологии «1С». Если продукты этой компании и раньше были популярными и востребованными, то сегодня они фактически стали базальтернативными.

Безусловно, есть ERP-системы и от других российских разработчиков, и многие интеграторы сейчас работают над созданием собственных решений. Но объективно ту часть рынка, которую занимала SAP, начинает занимать «1С». К тому же с 1 января 2025 г. государственные компании и объекты критической инфраструктуры должны отказаться от западного софта окончательно. А с 31 марта текущего года им запрещено покупать зарубежное ПО без соответствующего согласования. Это тоже добавляет очки популярности «1С».

Компании отказываются от использования продуктов не только SAP, но и Microsoft: Microsoft Dynamics Navision, Microsoft Axapta и других востребованных в свое время систем. Это связано, во-первых, с невозможностью по-

лучить качественную техническую поддержку, а во-вторых, с риском потерять деньги, если вендор решит разорвать контракт досрочно. Никому ведь не хочется купить лицензию на год, а в итоге пользоваться ею всего два месяца.

Управление корпоративными услугами

Импортозамещение коснулось и Service Desk – систем для управления ИТ-инфраструктурой. Сейчас мы наблюдаем буквально массовый исход вендоров таких западных решений как Jira, HPSM, Zendesk, Ivanti и SMAХ. На фоне их ухода заказчикам требуется автоматизация работы с заявками. Импортонезависимые продукты для выполнения таких задач, уже зарекомендовавшие себя на рынке, – это либо входящие в реестр российского ПО (например, Naumen), либо open source-решения.

Один из наших заказчиков – крупный российский вуз – долгое время использовал Jira для обработки заявок от преподавателей и студентов. По понятным причинам потребовалось заменить систему на отечественный продукт. Мы предложили импортонезависимое решение OTRS на базе open source. С его помощью вуз может, как и раньше, ежемесячно обрабатывать более 10 тыс. пользовательских заявок. В системе одновременно работают 100 исполнителей.

Между тем системы Service Desk применяют не только для решения ИТ-задач. Зачастую они служат единым сервисным окном для получения справок по форме 2-НДФЛ, оформления отпусков, расчета оставшихся рабочих дней и т.д. По сути, программные решения, удовлетворяющие подобные запросы, объединены в ESM-направление (Enterprise Service Management). Они востребованы во многих крупных российских компаниях и до недавнего времени базировались на западных технологиях, например Ivanti.

Весной потенциальные и действующие пользователи известных платформ столкнулись с тем, что заранее подготовленные контракты с иностранными вендорами оказалось невозможно оплатить из-за ограничения финансовых транзакций с Россией. Условия изменились, и компании вынуждены искать новые продукты. Это могут быть как российские системы, так и независимые open source-платформы.

Замена OCR-продуктов

Распознавание документов – частая задача в общих центрах обслуживания. Для ее решения в крупных организациях нефтегазового сектора, ретейла, телекома используют различные технологии. И российские аналоги зарубежных OCR-систем сейчас тоже весьма востребованы.



Тренинговый центр АНО КС ЦОД

Открой новое пространство знаний о ЦОДах!

Расписание программ на 2022-23 гг.

ПОСТРОЕНИЕ ЦОД

16–18 ноября, 2022, Москва

10–12 апреля, 2023, Москва

ЭКСПЛУАТАЦИЯ ЦОД

13–15 декабря, 2022, Москва

26–28 июня, 2023, Москва

ЭЛЕКТРИЧЕСКИЕ И МЕХАНИЧЕСКИЕ СИСТЕМЫ ЦОД

1–3 марта, 2023, Москва

УПРАВЛЕНИЕ ПРОЕКТИРОВАНИЕМ И СТРОИТЕЛЬСТВОМ ЦОД

17–19 мая, 2023, Москва



Специусловия при прохождении
онлайн-курсов

Подробнее уточняйте по email :
info@ano-dcc.ru

16+

Реклама

ano-dcc.ru

Преподаватели курсов — эксперты отрасли ЦОДов, обладающие многолетним практическим опытом, за плечами которых создание и эксплуатация крупнейших российских объектов.

Описание и регистрация
ano-dcc.ru/study/



Они основываются либо на открытых движках распознавания, либо на тех, которые не привязаны к иностранным сервисам.

Как правило, распознавание требуется для обработки первичной бухгалтерской документации, кадровых и неструктурированных документов и анкетных форм, заполненных от руки. Чаще всего компании использовали решения Kofax, ABBYY, IBM Datacap. Первые два были наиболее популярными в России, а теперь у их пользователей возникают проблемы с оплатой лицензий и невозможностью использовать западное ПО в госструктурах.

Напомню, что продукты исторически российской компании ABBYY с января 2022 г. перестали быть отечественными. А поскольку доля разработчика на рынке была огромная, мы сейчас фиксируем огромный же спрос на замену технологий ABBYY.

В качестве альтернативы предлагаем клиентам различные решения как на основе платформ роботизации процессов, так и заточенные именно на распознавание документов, например, EasySeparate. Это разработка российских специалистов, и она также включена в единый реестр ПО.

Меняем иностранных роботов на отечественные

С уходом европейских разработчиков возникает риск остановки проектов роботизации процессов. До сегодняшнего дня российские компании использовали три крупнейшие мировые платформы – Blue Prism, UiPath и Automation Anywhere. Их роботы в основном были доступны по подписке, и сейчас заказчики спешно ищут им замену.

На этом направлении мы также наблюдаем повышенный спрос на миграцию на российские платформы, скажем, на Sherpa RPA или Robin. Вкупе с поддержкой опытных консультантов эти платформы смогут функционально заменить соответствующее иностранное ПО.

Во всех перечисленных сферах и проектах российские технологии проявляют себя на уровне западных аналогов. Будут ли проблемы с их внедрением и использованием – зависит исключительно от квалификации исполнителя. Поэтому рекомендую искать интегратора с опытом в нужном направлении, готового сделать обзор выбранной платформы и помочь разобраться в ее функциональности.

К слову, по стоимости российские решения либо сопоставимы с иностранными, либо дешевле, поэтому вполне конкурентоспособны и вписываются в бюджеты компаний.

Безусловно, крупные западные решения пока продолжают работать, и поддерживаемые ими процессы не остановятся в один момент, но правильно оценить возможные риски и начать переход на отечественные аналоги лучше без лишних проволочек. **ИКС**



**СВОБОДНЫЕ
ТЕХНОЛОГИИ
ИНЖИНИРИНГ**

ПРОСТЫЕ РЕШЕНИЯ СЛОЖНЫХ ЗАДАЧ

**ПРОЕКТИРОВАНИЕ
И СТРОИТЕЛЬСТВО
ДАТА-ЦЕНТРОВ**

Реклама



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

+7 (495) 120-28-66

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

От чего зависит стоимость проектирования и строительства ЦОДа?

Андрей Павлов, генеральный директор, «ДатаДом»

Самый частый вопрос, который, собираясь строить ЦОД, нам задают начинающие инвесторы: «Сколько стоит?». И мы регулярно видим недоумение на их лицах, когда отвечаем, что затрудняемся сказать без уточнения деталей, или называем широкий диапазон цен в расчете на одну стойку.



В данном вопросе, как и во многих других, экспертных знаний недостаточно. Можно провести аналогию с автопромом. Невозможно однозначно ответить, сколько стоит автомобиль, если неизвестно, идет ли речь о грузовике, легковушке, спецтранспорте или электромобиле. В зависимости от мощности двигателя, марки, комплектации цены могут различаться в десятки раз.

В этой статье постараемся описать основные моменты, определяющие стоимость проектирования и строительства ЦОДа.

Стоимость проектирования

Инженерные системы, основанные на разных технологиях, требуют разных трудозатрат при проектировании. Например, проектирование системы холодоснабжения на фреоне гораздо проще, нежели на жидком хладагенте. В первом случае внешние и внутренние блоки соединяются прямой трассой, а во втором необходимо разрабатывать гидравлическую схему; появляется множество дополнительных устройств: задвижек, клапанов, теплообменников, насосов; труднее разрабатывать и реализовывать желаемую схему резервирования. Еще труднее может оказаться проектирование системы холодоснабжения на прямом или косвенном фрикулинге, поскольку потребуется значительно более сложная автоматика, не нужная в первом случае.

Технология прокладки трасс коммуникаций между единицами оборудования ощутимо влияет на стоимость проектирования. Скажем, между трансформаторной подстанцией (ТП), ДГУ и ГРЩ, а также между чиллером и внутренними блоками системы охлаждения трассы могут пролегать по фасаду в лотках, по земле, под землей в колодце и по эстакаде. Трудозатраты на проектирование каждого из этих вариантов существенно различаются. Кроме того, длина трассы также напрямую влияет на стоимость проектирования.

Выбор системы электроснабжения в зависимости от используемого напряжения (20, 10, 6 кВ) может изменить общую стоимость проектирования, так как может потребоваться разработка дополнительных проектов РТП, ТП, трасс внешнего электроснабжения. На стоимость этих разделов также влияет длина трассы.

Время автономной работы ДГУ, зафиксированное в техническом задании, может потребовать включения в проект дополнительных разделов. Так, для небольших объектов автономная работа до 8 ч реализуется установкой бака необходимой емкости в контейнере рядом с дизель-генератором. Но если надо обеспечить работу в автономном режиме в течение 12 или

24 ч, то с высокой долей вероятности нужно будет разработать дополнительные архитектурно-конструктивные и инженерные разделы (автоматика, электроснабжение, технологические решения и т.д.).

Место размещения ДГУ. Самый простой вариант проекта предусматривает размещение мобильного ДГУ на шасси на внешней площадке. Однако этот вариант может не соответствовать требованиям законодательства, и зачастую он выполняется на страх и риск заказчика. Если ДГУ реализуется как стационарная установка на фундаменте, потребуется разработать систему газовыхлопа и дополнительный раздел охраны окружающей среды (ООС), что также означает увеличение трудозатрат. Кроме того, может потребоваться согласование раздела ООС в надзорных органах. Если же ДГУ располагается в помещении, то нужно спроектировать системы вентиляции, кондиционирования и внутреннего топливоснабжения установки, так как в случае контейнерного варианта эти подсистемы являются частью данного контейнера.

Допустимая нагрузочная способность перекрытий тоже может повлиять на стоимость проектирования: при отсутствии информации о ней потребуется провести дополнительные изыскания для ее определения, а если нагрузочная способность недостаточна (менее 1000 кг/кв. м), необходимо будет разработать проект усиления перекрытий.

Выполнение необязательных разделов проектирования по желанию заказчика (в случае разработки проектов не в объеме капитального строительства, согласно Постановлению Правительства РФ от 16.02.2008 № 87) увеличит трудозатраты, а следовательно, и стоимость проектирования. В число таких разделов входят: программа и методика испытаний (ПМИ), проект организации строительства (ПОС), охрана окружающей среды (ООС), сметный раздел в государственных расценках, ведомость объемов работ (ВОР) и т.д. Существенных трудозатрат может потребовать и эксплуатационная документация, особенно при большой глубине проработки.

Создание проектной документации в 3D-среде, с использованием BIM-технологий, также сказывается на стоимости проектирования. При этом надо обязательно учитывать степень детализации (LOD100 – LOD600).

CFD-моделирование распределения потоков воздуха для высоконагруженных и архитектурно сложных объектов помогает снизить вероятность ошибок при проектировании системы кондиционирования, но увеличивает стоимость проектирования.



Разработка полноценной двухстадийной документации (П и Р) требует больших трудозатрат. Этот вариант необходим в случае капитального ремонта, нового строительства или строительства, ведущегося на государственные деньги. В то же время для объектов, реализуемых в существующих зданиях, зачастую достаточно разработать одностадийную документацию, касающуюся архитектурно-планировочных решений и инженерных систем.

Проработка нескольких вариантов эскизного проекта и расчета технико-экономических показателей объекта (при наличии в техническом задании вариативности в выборе технологий электро- и холодоснабжения ЦОДа) обусловит дополнительные трудозатраты проектировщиков.

Планируемое количество киловатт на одну стойку существенно влияет на стоимость проектирования. С ростом мощности стойки не только увеличатся мощность инженерных систем и площадь для их размещения, но может потребоваться кардинальное изменение инженерных систем и применение более технологичных систем кондиционирования.

Количество, площадь и высота вспомогательных строений и помещений и состав инженерных систем в них также оказывают влияние на стоимость проектирования.

Стоимость проектирования внешних сетей без детального изучения объекта и документации оценить очень сложно. Отсутствие данных о внешних сетях повлечет за собой значительные трудозатраты, вплоть до выполнения инженерных и строительных изысканий на объекте. С достаточной точностью можно оценить стоимость проектирования ЦОДа внутри контура имеющегося или строящегося здания.

Наконец, **согласование в надзорных органах, сопровождение при экспертизе и сер-**

тификации объекта существенно отражается на стоимости проектных работ.

Стоимость строительства

Средняя мощность, потребляемая одной стойкой, – главный параметр, определяющий затраты при строительстве. Многие заказчики просят назвать стоимость ЦОДа на 100 стоек по 6–7 кВт на стойку. Между тем разница в мощности систем холодоснабжения и электроснабжения для вариантов 6 и 7 кВт составляет ровно 20%. В общем случае стоимость строительства ЦОДа практически линейно зависит от мощности на стойку. Безусловно, при увеличении мощности на 1 кВт стоимость некоторых систем, в частности, систем безопасности, пожарных систем, СКС, ЛВС, а также строительной подготовки изменится незначительно, но поскольку на системы холодо- и энергоснабжения приходится до 60% бюджета строительства ЦОДа, подобное изменение может повлечь за собой увеличение стоимости на 15–20%.

Выбор технических решений инженерных систем напрямую влияет на стоимость строительства ЦОДа. Например, фреоновая система кондиционирования может оказаться до двух раз дешевле, чем чиллерная система с фрикулингом или система на прямом или косвенном фрикулинге. Аналогичная ситуация с выбором вариантов системы энергоснабжения – разница в стоимости связки ИБП + ДГУ и ДИБП существенна и зависит от масштаба объекта и выбранной схемы резервирования. Литий-ионные АКБ значительно дороже свинцово-кислотных. Еще один показательный пример влияния технологий на стоимость – разница в стоимости реализации трасс электроснабжения на шинопроводах и на кабельной продукции.

Выбор поставщиков и моделей инженерного оборудования. Есть целый перечень вен-

доров ИБП, ДГУ, систем кондиционирования, стоек, PDU – российских, китайских, европейских, американских. В зависимости от сложности логистики, курсов валют, раскрученности марки, применяемых схемотехнических решений, надежности и наличия дополнительных технологических преимуществ (КПД, глубина мониторинга, масштабируемость, автоматизация и т.д.) стоимость похожих по мощности единиц инженерного оборудования может различаться в несколько раз.

Стоимость реализации системы мониторинга сложно оценить точно, так как она напрямую зависит от количества отслеживаемых параметров. К примеру, система, контролирующая только вводные автоматы в ГРЩ, может быть в несколько раз дешевле, чем система, которая управляет каждой розеткой в стойке. Стоимость обычного PDU составляет от 10–25 тыс. руб., а PDU с возможностью мониторинга и управления – в среднем \$1000–2000 тыс., и таких блоков в каждую стойку понадобится два.

Аналогичная ситуация складывается и с СКС и ЛВС. Коммерческие ЦОДы либо вовсе не реализуют СКС, только закладывают в проект лотки под нее и кроссовые стойки, либо прокладывают лишь по два оптических кабеля на рядную кроссовую стойку. Напротив, в банковской сфере принято на этапе строительства создавать полноценную СКС, закладывая по 24–48 портов «меди» и оптики на каждую стойку. И в зависимости от производителя стоимость такой системы может составить до 30% бюджета ЦОДа.

Уровень резервирования инженерных систем ЦОДа оказывает на стоимость строительства критическое влияние. Смена схемы резервирования систем кондиционирования и электроснабжения с N + 1 на 2N может изменить общую стоимость строительства ЦОДа на 10–30%.

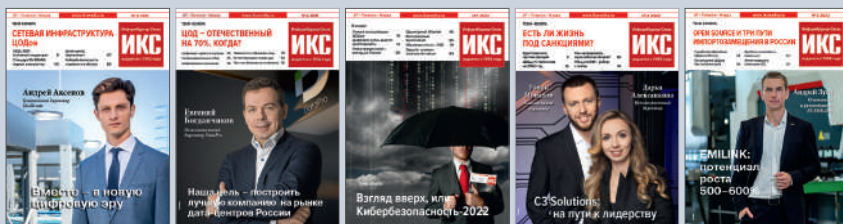
Гринфилд или браунфилд. Безусловно, стоимость строительства ЦОДа зависит от того, строится объект в имеющемся здании или в «чистом поле». Кроме того, даже внутри имеющегося здания объем работ может быть разным – в одном случае возведение кирпичных перегородок, выравнивание пола и покраска стен, в другом случае снос капитальных перегородок, усиление перекрытий и восстановление фасада. Стоимость нового строительства также может существенно различаться: одно дело построить быстровозводимое одноэтажное здание из сэндвич-панелей с несущей кровлей, совсем другое – здание из монолита в несколько этажей, с дизайнерскими фасадами и кровлей, на которой будут располагаться ДГУ и чиллеры.

Как и на проектные работы, на стоимость строительства влияет **время автономной работы ДГУ**, так как большая автономия требует создания крупных топлиохранилищ, оснащенных системами автоматики, безопасности, очистки, слива топлива, насосами и т.д.

Место расположения ДГУ/ДИБП также влияет на стоимость. Может потребоваться реализация систем вентиляции и кондиционирования, пожаротушения, слива топлива, газовой хлопа, шумоглушения и многих других.

На стоимости строительства существенно отражается необходимость (или отсутствие таковой) **модернизации или установки новой ТП**, а также длина трассы до ГРЩ, ее сложность и способ прокладки. То же самое относится к трассам всех других инженерных систем.

Мы перечислили основные моменты, влияющие на стоимость проектирования и строительства ЦОДа. Но ЦОД, как правило, объект уникальный, и нельзя исключить возникновение в каком-нибудь конкретном случае дополнительных факторов влияния. **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
[Подробнее см. на сайте](#)

Как строить ЦОДы в условиях санкций

В сентябре компания IXcellerate открыла свой третий дата-центр в России, который должен стать частью крупнейшего коммерческого кампуса ЦОДов в Европе. О проекте рассказывает Сергей Вышемирский, технический директор IXcellerate.



– Строительство ЦОДа MOS5 велось в непростых условиях: пандемия, санкции... Какими были главные трудности и как вы их преодолели?

– Мы в санкционном режиме живем с 2014 г., приспособились к нему и спокойно работали. Ощутимые коррективы в нашу жизнь внесла пандемия, которая повлекла за собой нарушение сроков поставок. Если раньше мы рассчитывали на три, максимум шесть месяцев с момента заказа, то в 2020 г. сроки выросли до 12 месяцев и более. Большинство западных вендоров увеличили сроки поставок практически вдвое. Вот к этому адаптироваться было уже намного сложнее, ведь планы строительства никто не менял! Потом в Суэцком канале застрял контейнеровоз, и все мировые логистические цепочки нарушились снова. Цены на контейнерные перевозки взлетели, следом – цены на оборудование и стоимость проектов в целом.

Эти катаклизмы повлекли за собой ощутимый на мировом уровне дефицит чипов, которые используются во всех моделях холодильного оборудования. Каждый вентилятор имеет свой «головной мозг», который подстраивается под команды контроллера чиллера; это высокотехнологичная конструкция, работа которой напрямую зависит от чипов. Из-за того, что сроки поставок сдвинулись, вся индустрия холодоснабжения оказалась на голодном вентиляторном пайке. Из этой ситуации у производителей было два выхода. Первый – возвращаться на старые технологии, например, на внешний частотный преобразователь для регулирования скорости вращения вентилятора вместо «умного» встроенного микрочипа. Но такое решение снизило бы эффективность работы чиллера, по-

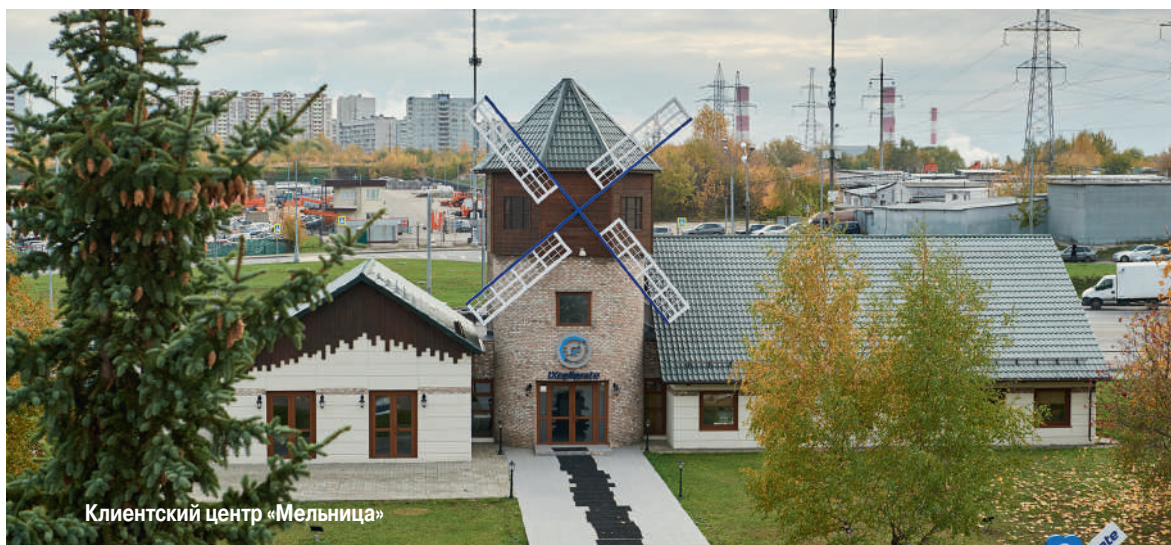
этому поставщики пошли по другому пути – они увеличили сроки поставок готового оборудования.

Справиться с этой проблемой нам помогло давнее стратегическое партнерство с вендором – одним из мировых лидеров по производству критически важной инфраструктуры для ЦОДов. Он присвоил заказам IXcellerate повышенный приоритет и отгружал оборудование в более короткие сроки. Для оптимизации строительных работ мы перешли на модульную сдачу проекта, закрывали этапы последовательно по мере поступления готового оборудования. В итоге оба новых машзала были запущены в плановые сроки. Первый – в декабре 2021 г., второй – в марте 2022 г.

– Проектное значение PUE нового ЦОДа ниже 1,3. Это значительно лучше среднемирового показателя (1,57 по данным Uptime Institute за 2021 г.). За счет чего планируете добиться такого PUE?

– Экономия достигается за счет применения энергоэффективных решений. Мы используем в системе охлаждения чиллеры с фрикулингом и подбираем их на несколько большую мощность, чем нужно. Благодаря этому добиваемся наиболее энергоэффективного режима с точки зрения нагрузки. Дело в том, что самый большой расход электричества требуется на предельных режимах работы оборудования, когда вентилятор задействует 100% своей мощности. Чем выше скорость вращения лопастей, тем больше нужно электричества. Но между скоростью и энергозатратами зависимость не линейная: если снизить скорость вращения на 20%, прибор будет потреблять электричества существенно меньше.





Клиентский центр «Мельница»

То же самое с теплообменниками и конденсаторами. Таким образом, благодаря переразмериванию мы снижаем максимальные нагрузки на компрессоры и продлеваем срок службы охлаждающего оборудования, а заодно экономим электричество.

Второе наше ноу-хау – температурный режим. Установленное в ЦОДе оборудование может работать при уличной температуре +38°C, что выше, чем рекомендуют в ASHRAE и Uptime Institute. На случай повышенных температур чиллеры оборудованы комплектами с адиабатическим предохлаждением, что позволяет в летние периоды снижать температуру воздуха на входе в чиллер на 10–15°C. Если на улице, допустим, +40°C, то на входе в чиллер мы будем иметь +25–30°C. Адиабатика обеспечивает повышение энергоэффективности при минимальном расходе воды.

На площадке Северного кампуса у нас уже были установлены комплекты для предохлаждения чиллеров. Когда мы включаем предохлаждение, энергопотребление системы холодоснабжения снижается на 5%. На уровне всего ЦОДа это огромная экономия.

– **Какие еще принципиально новые технические решения были использованы в ЦОДе MOS5 для повышения его энергоэффективности?**

– 85% всей энергоэффективности зависит от системы охлаждения – ее настроек и параметров. Чтобы повысить энергоэффективность, мы переразмерили мощность оборудования, повысили температуру холодоносителя, а также перешли на практически круглогодичный режим фрикулинга, совмещенного с использованием адиабатики.

Следуя мировым тенденциям, мы стали работать на горячей воде, повысив температуру холодоносителя в системе. Если на первом нашем объекте в кондиционеры подавалась вода с тем-

пературой 10°C, а возвращалась обратно с температурой 17°C (дельта 7°C), то сейчас мы применяем технологию «холодная стена», которая позволяет использовать температурный график 18/28 (дельта 10°C).

Чем ниже температура на улице, тем выше процент фрикулинга. На 100%-ный фрикулинг мы переходим при температуре +10°C. Совмещенный режим фрикулинга обеспечивает экономию, начиная с температуры +26°C, а так как у нас есть адиабатическая система предохлаждения, мы теоретически можем использовать частичный фрикулинг, даже если на улице +30°C. Таким образом, мы выходим практически на круглогодичный режим совмещенного фрикулинга и работаем на одних компрессорах не более трех месяцев в году. Благодаря такому подходу проектное среднегодовое значение PUE снижается до 1,3.

На экономию электричества также работают зальные кондиционеры, которые за счет низкой скорости воздуха и большой площади теплообменника потребляют значительно меньше электричества, чем классические кондиционеры с выдувом под фальшпол.

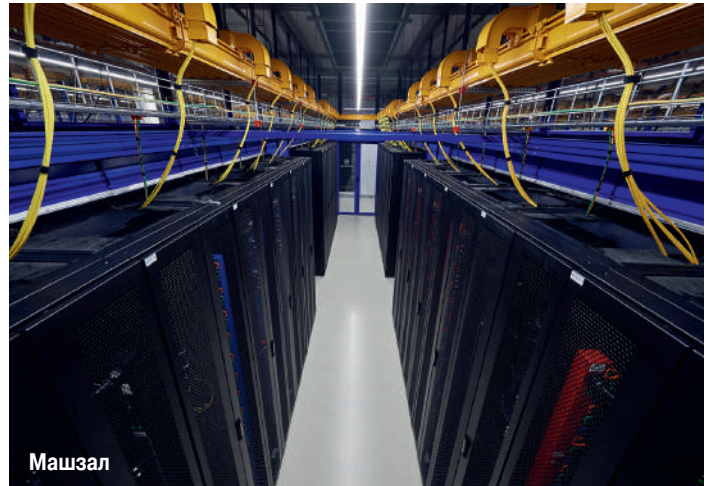
– **Почему в MOS5 использованы сразу несколько технологий пожаротушения: на базе тонкораспыленной воды и газа Novac 1230?**

– Технология пожаротушения выбирается клиентом. Пока не все готовы переходить на тонкораспыленную воду, поэтому мы сделали универсальное решение, которое позволяет использовать и дистиллированную воду, и газ – на выбор клиента. Если мы знаем, какой клиент к нам придет в тот или иной зал, – устанавливаем то, что ему нужно, если нет, ставим по умолчанию водяное тушение. Это вопрос гибкости нашего сервиса.

– **В свое время IXcellerate реализовала крупнейший машзал (около 1000 стоек). Почему на новом объекте залы поменьше?**



Энергомодули ЦОДа



Машзал

– Это также связано с гибкостью нашей сервисной политики и индивидуальным подходом к требованиям заказчиков. В дата-центре MOS5 мы уменьшили площадь помещений и разделили один большой машзал (1600 стойко-мест) на несколько мелких, чтобы иметь возможность использовать в них газовую систему пожаротушения.

– Вы уже давно и успешно применяете литий-ионные батареи. Каковы их основные преимущества? Что показали несколько лет эксплуатации?

– Основное преимущество – это занимаемая площадь. Помещения для хранения таких батарей не требуют супермощной системы охлаждения, достаточно простой вентиляции. Литий-ионные батареи можно размещать в одном помещении с ИБП, в то время как свинцовые всегда требуют отдельной локации и обустройства систем охлаждения и вентиляции.

Срок службы у литий-ионных батарей дольше: за время эксплуатации мы не сменили ни одной, в отличие от свинцовых – там каждые полгода выбраковывается одна-две. Плюс у

«лития» есть онлайн-мониторинг, позволяющий предотвращать вероятностные отказы.

По цене литий-ионные батареи стали доступнее. Это происходит за счет появления новых поставщиков и увеличения производства литиевых батарей. Драйвер роста – автомобильная индустрия (электрокары). Мир переходит на «зеленые» технологии, и мы вместе с ним.

Раньше использование литий-ионных батарей сдерживалось тем, что при возгорании они выделяют кислород, который поддерживает горение. Но сегодня эта проблема уже практически решена. Мы, например, используем батареи Samsung, в которых объем выделяемого кислорода сведен к минимуму.

Что касается утилизации – да, технология пока не разработана. Но я думаю, что вскоре должны создать технологию реанимации литий-ионных батарей, чтобы иметь возможность использовать их повторно, а не выбрасывать. Эти батареи «умные», у них внутри много всякой электроники, и отправлять их в утиль дорого.

– Основные инженерные системы MOS5 производства западных вендоров. Как в нынешних условиях будут происходить их обслуживание, ремонт, модернизация? Имеется ли необходимый ЗИП?

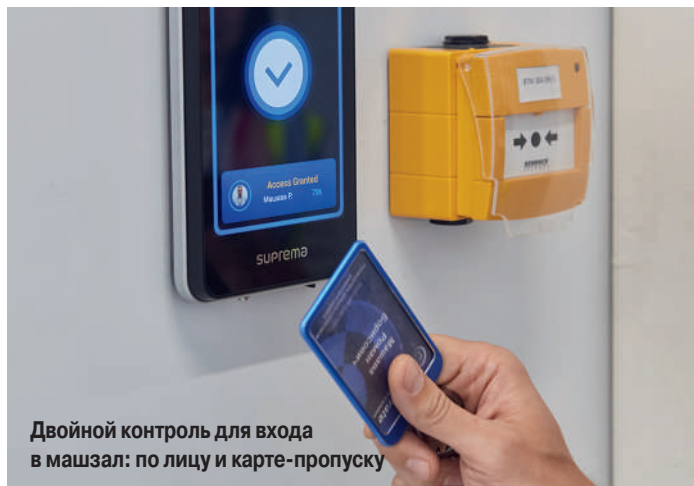
– Обслуживание выполняют те же компании, что и раньше. Наша сервисная служба проводит ТО и поддерживает эксплуатацию многих элементов своими силами, что положительно сказывается на бюджете. Модернизация ИБП, чиллеров, кондиционеров не предполагается. Нам она не нужна, потому что в iXcellerate всегда приобретали новые модели, которые только выходили на рынок, а некоторые даже разрабатывались специально по нашему запросу, как это было, например, с технологией «холодная стена» от Vertiv. Так же и чиллеры с адиабатическим предохлаждением – мы их получили еще в 2019 г., и новая линейка ИБП, в которой учтены и устранены все старые погрешности.



Центр мониторинга и управления



Система пожаротушения



Двойной контроль для входа в машзал: по лицу и карте-пропуску

Согласно политике IXcellerate, все запчасти должны находиться под нашим контролем, поэтому при покупке оборудования мы всегда приобретаем запчасти с большим запасом. Мы обеспечены ЗИП на ближайшие пять лет. В случае непредвиденных ситуаций будем увеличивать закупки за счет как импорта, так и перехода на локальные решения от российских производителей.

– Какие российские решения использованы в ЦОДе MOS5?

– Это трансформаторные узлы/системы, «умные» PDU, зальные блоки распределения питания, серверные шкафы, системы герметизации горячих и холодных коридоров, телекоммуникационные лотки, переключатели и другие элементы для электрической коммутации. Таких решений становится все больше, но надо отметить, что на работу с российскими поставщиками требуется больше времени. Мы проводим тщательный отбор и дополнительное тестирование всех решений, так как для нас самое важное – качество и надежность.

– В каких сегментах российские производители предлагают конкурентные продукты?

– Это системы безопасности, пожаротушения, видеонаблюдения и контроля доступа. В этих сегментах можно смело использовать российское ПО. Недавно появились даже аналоги технологии тушения тонкораспыленной водой – их стали выпускать сразу три российских предприятия. По качеству они несколько не уступают зарубежным.

После ухода многих международных поставщиков оказалось, что некоторые из них (например, производители фальшпола) уже давно использовали в своих решениях российские компоненты. А отдельные элементы инфраструктуры, такие как контроллеры, кабельные лотки, несущие системы, еще до санкций были полностью заменены нами на российские.

Российские аналоги могут составить конкуренцию по своей технологичности и качеству в

сегменте кондиционеров, как фреоновых, так и фанкойлов. Проигрыш будет только в цене: российские дороже за счет ручной сборки (на Западе трудозатраты ниже благодаря автоматизации сборочных процессов).

– По каким позициям придется, как и раньше, ориентироваться на зарубежных вендоров?

– На рынке ЦОДов самая сложная ситуация с отсутствием российских аналогов в сегменте ДГУ и чиллеров большой мощности. В России пока не производятся решения для таких крупных дата-центров, как IXcellerate.

– Какие новые технологии присматриваете для своих ЦОДов?

– Я вижу необходимость переходить на «зеленые» технологии и более мощные накопители энергии, которые позволят минимизировать использование дизелей в работе дата-центров. Иначе рано или поздно все коммерческие ЦОДы с большой энергоемкостью превратятся в аналог машинно-тракторной станции. За десять лет у нас, например, не было ни одного отключения от городской электросети, но отказаться от дизелей мы, согласно требованиям Uptime Institute, не можем. Если какой-нибудь глобальный коллапс все же случится, то запасов топлива все равно хватит не более чем на 12 ч. На случай крупных форс-мажоров резервирование должно строиться за счет двух независимых фидеров, идущих разными лучами от реально независимых питающих центров. Например, если подключиться по второй категории к сети ФСК и к генерации «Газпрома» (ТЭЦ), то необходимость в дизелях на всю мощность ЦОДа отпадет.

Альтернативой бесконечному наращиванию дизельного парка может также стать индивидуальный подход к резервированию данных, как это делает большинство крупных западных ЦОДов: они не резервируют всех клиентов на 100%. Заказчик может выбирать: свои самые важные данные резервировать за счет ДГУ, а остальное – за счет размещения в другом ЦОДе. **ИКС**

Выбор оптимальной концепции охлаждения майнингового ЦОДа

Григорий Юдин,
технический директор;
Анастасия Кузнецова,
главный специалист по механическим системам, DCConsult

Представьте, что вам необходимо создать систему охлаждения для майнингового ЦОДа с ИТ-мощностью 200 МВт. Как организовать воздухообмен на таком объекте?

Именно с таким нестандартным запросом обратился к нам заказчик.

Наша задача как консультантов состояла в анализе уже предложенных для объекта инженерных решений, их коррекции и дополнительной проверке на основе нашего опыта и с применением CFD-моделирования воздушных потоков.

Разумеется, мы представляем себе все достоинства и особенности стремительно набирающего популярность иммерсионного охлаждения, однако в данном проекте по целому ряду причин задача охлаждения майнеров должна была решаться именно обдувом воздухом.

Конструктивные особенности майнеров

Майнеры, производимые ведущими компаниями, можно разделить на две основные группы – устройства на базе специализированных чипов (ASIC) и на базе графических ускорителей (GPU). С точки зрения охлаждения они различаются незначительно. Вместе с тем в отличие от серверного оборудования, которое снабжено сервисным процессором, осуществляющим диагностику состояния устройства, измерение температуры, управление вентиляторами и пр., сервисный процессор майнера существенно упрощен и слу-

жит для настройки майнера и его подключения к планировщику заданий. Таким образом, система управления продувкой сведена к абсолютному минимуму, и вентиляторы все время работают на полных оборотах.

Что представляет собой один из наиболее популярных майнеров ASIC AntMiner S19 Pro в цифрах? На скромные габариты 370 × 195,5 × 290 мм (Д × Ш × В) приходится 3,25 кВт постоянного тепловыделения. Допустимый для бесперебойной работы температурный диапазон – 0–40°C при относительной влажности воздуха не более 90% без выпадения конденсата. Установленные вентиляторы обеспечивают объемный расход воздуха порядка 700 куб. м/ч. Механическая фильтрация воздуха, поступающего на вход устройства, не предусмотрена, поэтому поддерживать рекомендуемые условия эксплуатации необходимо на уровне машинного зала.

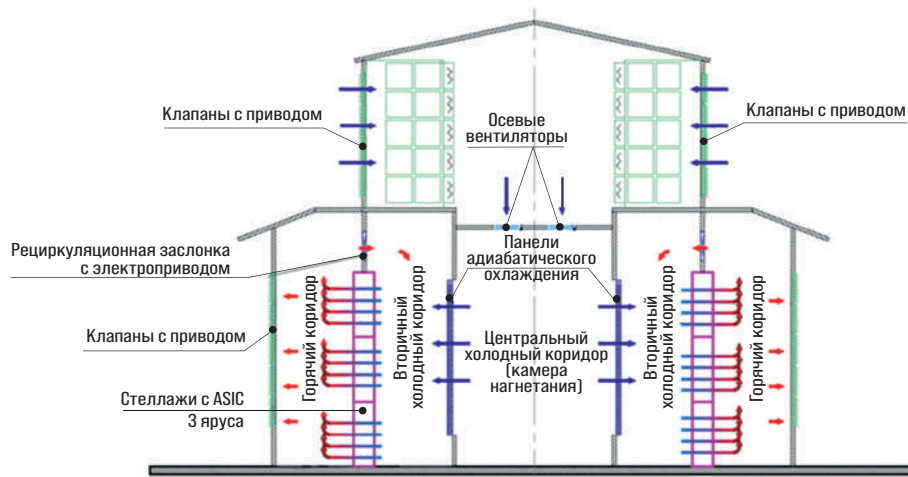
Искушенный в майнинге читатель скажет, что эти устройства работают в любых, самых жестких условиях. Согласны, это не бизнес-ориентированное ИТ-оборудование со своими SLA и заботой о доступности, но акцент сделаем на том, что в то время, когда майнер не работает, он не приносит ожидаемую прибыль, да и при массовых отказах устройств проявится нехватка обслуживающего персонала для восстановления работоспособности оборудования.

Каков он, ЦОД для майнинга?

Вернемся к проектируемому объекту, который был задуман в виде легковозводимого ангара. Предложенное нам для анализа проектное решение для охлаждения ЦОДа было следующим: наружный воздух после минимальной фильтрации с помощью нагнетающих осевых вентиляторов, расположенных в боковых стенах ангара, подавался в пространство холодных коридоров машинного зала. Нагретый майнерами воздух поступал в центральный горячий коридор, откуда отводился наружу вытяжными осевыми вентиляторами.



Рис. 1.
ASIC Bitmain
AntMiner
S19 Pro ▶



◀ **Рис. 2.**
Концепция майнингового ЦОДа с центральным холодным коридором

Изучив это решение, мы увидели, что оно обладает рядом недостатков, поскольку не учитывает следующие аспекты:

- повышенную запыленность вследствие близости выбранной для ЦОДа площадки к районам лесозаготовок и угольным развалам ГРЭС;
- высокую сейсмичность региона;
- высокие экстремумы (положительные и отрицательные) температуры наружного воздуха при низкой среднегодовой температуре.

Сведя исходные данные воедино, мы предложили альтернативную схему воздухообмена в ЦОДе. Так, в рамках уже сформированной архитектурной концепции ангара было решено организовать центральный холодный коридор в виде камеры нагнетания, куда очищенный фильтрами наружный воздух подается из верхней зоны ангара с помощью осевых вентиляторов (рис. 2). Далее после адиабатического охлаждения подготовленный воздух поступает во вторичные холодные коридоры для подачи к майнерам. Нагретый майнерами воздух попадает в горячие коридоры, откуда удаляется наружу или подается на рециркуляцию. Рециркуляция может быть полной или частичной в зависимости от температуры наружного воздуха.

Основные преимущества такой компоновки заключаются в существенном снижении нагрузки на систему фильтрации вследствие за-

бора воздуха из верхней части ангара, а также в уменьшении энергопотребления системы из-за отсутствия потребности в вытяжных вентиляторах.

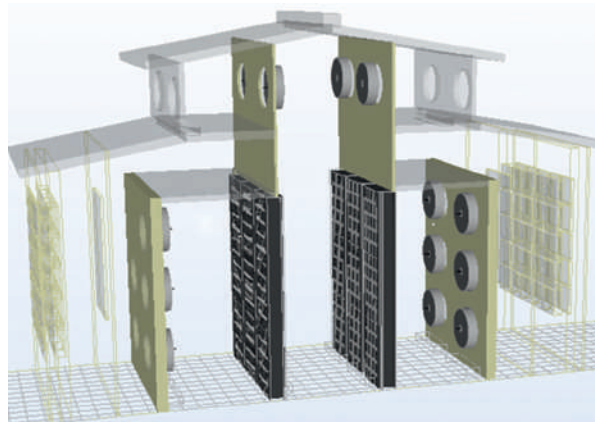
Что показало CFD-моделирование

Далее мы приступили к построению CFD-моделей обоих компоновочных решений, для того чтобы наглядно представить заказчику все их особенности.

Технология вычислительной гидрогазодинамики дает возможность безопасно и экономично проверить планируемые технологические решения на цифровом двойнике объекта. А верификация CFD-моделей, проводимая на уже построенных объектах, позволяет и нам, и заказчикам быть уверенными в точности прогнозов поведения окружения при конкретных нагрузках и настройках инженерных систем.

Поскольку геометрические размеры майнингового ЦОДа оказались значительны, для построения двух CFD-моделей была выбрана одна секция ангара. На рис. 3 и 4 представлены общие виды моделей секции ЦОДа: исходный вариант с общим горячим коридором и альтернативное решение с общим холодным коридором.

В список ключевых параметров, по которым предполагалось сравнивать две CFD-модели, мы включили:



◀ **Рис. 3.**
Общий вид модели секции майнингового ЦОДа с общим горячим коридором

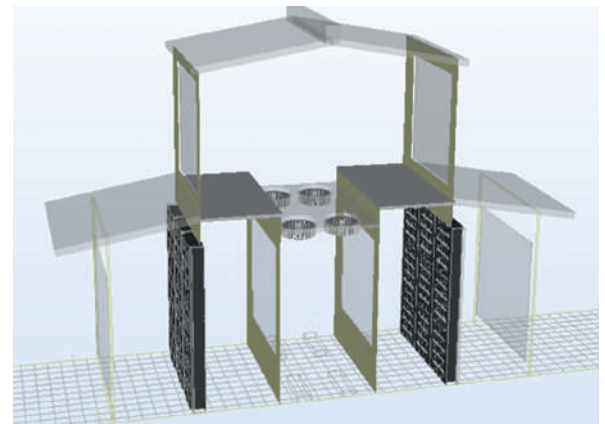
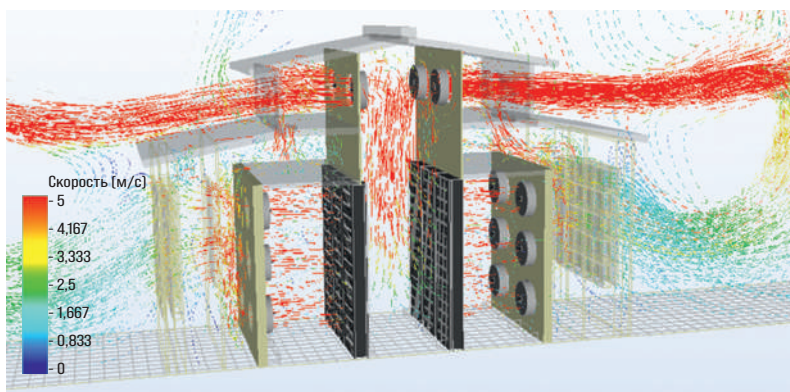
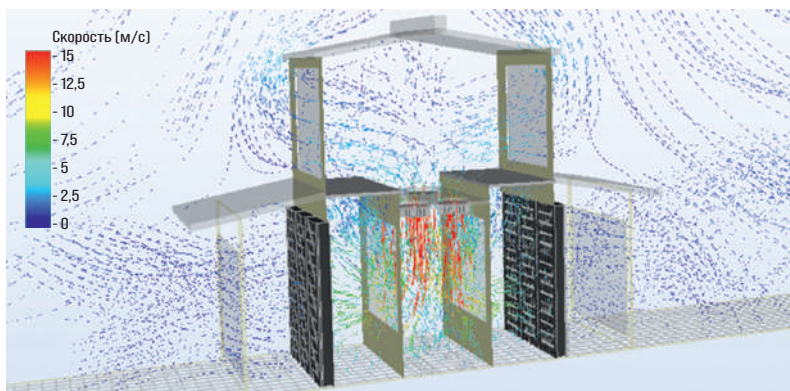


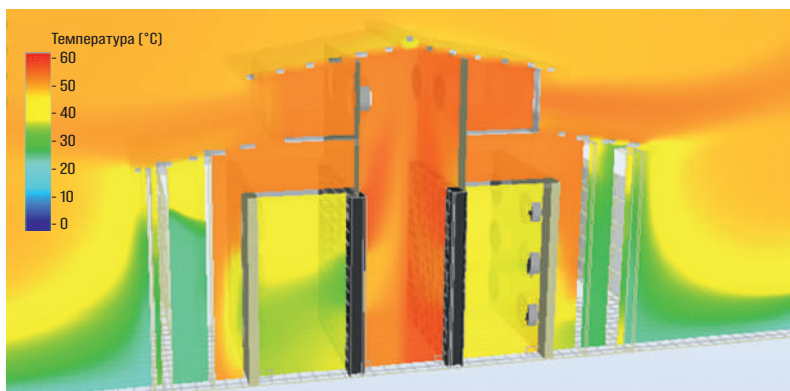
Рис. 4. Общий вид модели секции майнингового ЦОДа с общим холодным коридором ▶



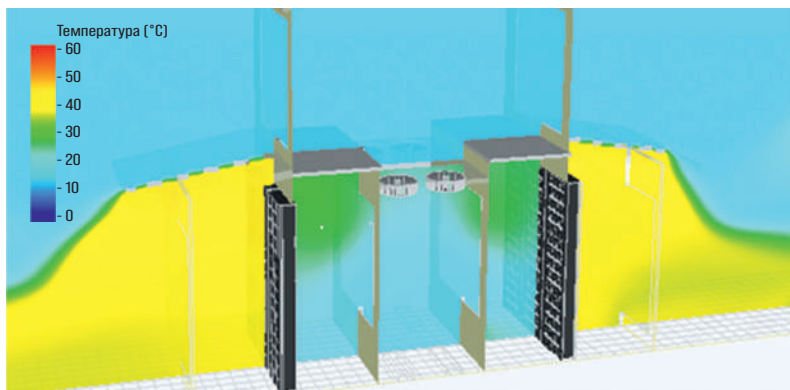
▲ Рис. 5. Карта распределения потоков воздуха для модели с общим горячим коридором



▲ Рис. 6. Карта распределения потоков воздуха для модели с общим холодным коридором



▲ Рис. 7. Карта распределения температур в вертикальной плоскости для модели с общим горячим коридором



▲ Рис. 8. Карта распределения температур в вертикальной плоскости для модели с общим холодным коридором

- обеспечение требуемого объемного расхода воздуха;
- перепад давления на фильтрах;
- отсутствие закливания выбрасываемого воздуха на воздухозабор;
- потребность в вытяжных вентиляторах;
- ремонтпригодность;
- удобство обслуживания системы фильтрации.

На картах распределения потоков воздуха (рис. 5 и 6) ясно видно, что в модели с общим горячим коридором ярко выражено закливание выбрасываемого воздуха в области воздухозабора.

Закливание выбрасываемого воздуха приводит к дополнительному нагреву наружного воздуха в области воздухозабора. Этот эффект можно наблюдать на карте распределения температур модели с общим горячим коридором (рис. 7).

При этом в модели с общим холодным коридором карты распределения потоков воздуха и температур (рис. 6 и 8) показывают отсутствие закливания выбрасываемого воздуха и дополнительного нагрева наружного воздуха в местах воздухозабора. Стоит заметить, что внутри вторичных холодных коридоров воздух в верхней части более нагрет не только по причине конвективного разделения, но и вследствие эжекции в верхней части фильтров. Это явление следует учесть при подборе оборудования.

Анализ карт распределения параметров обеих CFD-моделей, а также эксплуатационных особенностей объекта позволил сделать вывод, что оптимальным решением для данного майнингового ЦОДа является компоновка с общим холодным коридором. Она обладает следующими преимуществами:

- отсутствие закливания выбрасываемого воздуха и, как следствие, отсутствие перегрева наружного воздуха в области воздухозабора;
- отсутствие потребности в вытяжных вентиляторах;
- снижение нагрузки на систему фильтрации;
- отсутствие необходимости балансировки воздухообмена нагрузки по сторонам сооружения;
- возможность поэтапного ввода оборудования.

Более того, опыт этого проекта свидетельствует о том, что чем раньше проводится анализ концептуальных решений, схем воздухообмена и компоновки объекта, тем больше узких мест в проекте можно обнаружить. А объединив усилия проектировщиков и CFD-моделирование, можно добиться оптимального результата. ИКС

Прямое жидкостное охлаждение: переход неизбежен

Изменения как в технических, так и в бизнес-требованиях подталкивают операторов ЦОДов к переходу на прямое жидкостное охлаждение. До его широкомасштабного внедрения предстоит преодолеть массу препятствий, но многие в отрасли полагают, что это лишь вопрос времени.

Охлаждение остается основной причиной неэффективности ЦОДов, поскольку на него расходуется много не только энергии, но и денег – на дорогостоящее оборудование. Между тем, после периода инноваций, в том числе оптимизации воздушных потоков и внедрения бескомпрессорных режимов отвода тепла, повышение эффективности охлаждения затормозилось. Согласно «Глобальному исследованию дата-центров», проведенному Uptime Institute в 2021 г., коэффициент энергоэффективности (PUE) в отрасли составляет 1,57 – это значительно ниже, чем 1,98 в 2011 г., но лишь немногим лучше рекордно низкого показателя 2018 г. – 1,58.

Прямое жидкостное охлаждение (Direct Liquid Cooling, DLC) – это совокупность методов, позволяющих отводить тепло от ИТ-электроники путем циркуляции жидкого хладагента. До недавнего времени применение жидкостного охлаждения ограничивалось в основном приложениями в области высокопроизводительных вычислений. Для таких вычислений характерны чрезвычайно высокая плотность инфраструктуры и высокоскоростные соединения между вычислительными узлами. В крупномасштабной ИТ-инфраструктуре DLC используют лишь отдельные ЦОДы, среди них – французский OVHcloud. В целом же даже в новых ЦОДах придерживаются воздушного охлаждения, поскольку оно хорошо изучено и в большинстве случаев достаточно эффективно.

Эксперты Uptime Institute Intelligence полагают, что скоро баланс сместится в сторону DLC. После многочисленных фальстартов и задер-

жек проектов крупных операторов интерес к прямому жидкостному охлаждению вновь усилился. Приложения, требующие высокоплотной инфраструктуры, распространяются все шире и становятся все более масштабными. К ним относятся аналитика на основе больших данных и быстро развивающиеся глубокие нейронные сети. Кроме того, от ЦОДов требуют дальнейшего роста эффективности и повышения экологичности, а резервы повышения эффективности воздушного охлаждения практически исчерпаны. По оценкам, даже максимально оптимизированные объекты тратят на воздушное охлаждение и сопутствующие потери не менее 15–20% энергии.

Похоже, что именно эволюция микроэлектроники для ЦОДов подтолкнет их операторов к массовому переходу на DLC. Мощность серверных чипов и, следовательно, мощность серверов будет расти. И речь идет не об отдаленном будущем. В Uptime Institute ожидают, что уже во второй половине 2020-х гг. повышение плотности и мощности массовых серверов и кремниевых микросхем постепенно сделает воздушное охлаждение непрактичным и даже убыточным как по капитальным, так и по операционным затратам.

Однако переход на прямое жидкостное охлаждение, несмотря на очевидную потребность в нем, осложняется рядом технических и экономических препятствий. В основе проблем – отсутствие стандартов на рынке DLC. В отличие от воздушного охлаждения, где воздух выступает и в качестве стандартной охлаждающей среды, и в качестве естественной границы между системами охлаждения и ИТ-системами, в

Дэниел Бизо, директор по научно-исследовательской работе;
Ленни Саймон, старший научный сотрудник;
Жаклин Дэвис, аналитик-исследователь, Uptime Institute Intelligence

жидкостном не существует аналогичного стандартного хладагента или границы.

Вендоры недостаточно координируют свои разработки DLC-платформ, в результате на рынке присутствует множество несовместимых систем с поддержкой от разных поставщиков ИТ-оборудования. В отсутствие стратегического подхода к созданию стандартов DLC, ЦОДам, возможно, придется применять несколько систем прямого жидкостного охлаждения, каждая со своими особенностями и ограниченной совместимостью, что увеличит эксплуатационные расходы и риски.

Впрочем, за последние годы системы DLC претерпели существенные изменения, их стало проще внедрять и эксплуатировать. Растущее количество инсталляций DLC дает поставщикам необходимую информацию для разработки более надежных, простых в использовании и совместимых по материалам продуктов.

Чтобы выяснить точку зрения игроков отрасли на DLC, эксперты Uptime Institute Intelligence в декабре 2021 – январе 2022 г. провели глобальный онлайн-опрос владельцев/операторов ЦОДов, их ИТ-менеджеров, а также проектировщиков ЦОДов и инженерных систем, консалтинговых фирм и поставщиков продуктов и услуг. В опросе Direct Liquid Cooling Survey 2022 приняли участие 197 операторов корпоративных ЦОДов.

Типы технологий DLC

Мы определяем DLC как широкую категорию методов, в которых охлаждающая жидкость подается к компонентам ИТ-системы (процессорам, памяти и другой электронике) для отвода тепла. Отвод может производиться как через радиаторы, так и при прямом контакте. Мы не будем касаться других систем, подающих жидкости в стойку (например, теплообменников на двери), поскольку в качестве промежуточной среды передачи тепла от ИТ-электроники к инфраструктуре охлаждения они используют воздух. Это не формальное разделение: технические и эксплуатационные характеристики таких систем существенно различаются.

В настоящем исследовании мы рассматриваем шесть основных типов технологических платформ DLC, которые делятся на две категории: построенные на базе охлаждающих пластин и иммерсионные (погружные) системы.

Системы с охлаждающей пластиной

Существуют три типа систем DLC с охлаждающей пластиной.

Пластины с водяным охлаждением. Очищенная вода, деионизированная вода или водно-гликолевая смесь циркулирует через охлаждающие пластины по замкнутому контуру

для отвода тепла от самых мощных (и самых горячих) компонентов – центрального и графических процессоров (или других ускорителей) и модулей памяти. Как правило, охлаждающие пластины поглощают 70–80% общей тепловой нагрузки сервера в зависимости от конфигурации и интенсивности его работы. Системы водяного охлаждения получили наибольшее распространение, поскольку давно используются в высокопроизводительных вычислениях, но в некоторых ЦОДах все еще опасаются утечек в ходе эксплуатации.

Охлаждающие пластины с однофазным диэлектрическим хладагентом. В этих пластинах вместо воды в качестве теплоносителя используется специальная диэлектрическая жидкость. Протечка такой жидкости не приведет к повреждению электроники, а ее инертность означает отсутствие коррозии внутренних материалов контура (охлаждающей пластины или теплообменника). По сравнению с водой эти жидкости имеют меньшую удельную теплоемкость, поэтому для той же холодопроизводительности нужна более высокая скорость потока, чем в пластинах с водяным охлаждением, что требует более высокого давления. Это относительно новое решение с ограниченным опытом эксплуатации.

Охлаждающие пластины с двухфазным диэлектрическим хладагентом. Диэлектрический хладагент закипает при относительно низких температурах (например, ниже 49°C) в камере охлаждающей пластины. Испаряющийся теплоноситель выводится из сервера по шлангам и проходит через конденсатор для рециркуляции. Большое количество энергии, поглощаемой при фазовом переходе (кипении и испарении), обеспечивает необходимую холодопроизводительность. Этот вариант лишь недавно стал доступен, но вызывает большой интерес в силу высокой эффективности, низких рисков и относительной простоты внедрения.

Иммерсионные системы

Существуют также три типа иммерсионных (погружных) систем DLC.

Погружное шасси (однофазное). Каждый сервер заключен в герметичный, автономный корпус. Иногда несколько компактных серверных узлов устанавливаются в одно шасси. Внутри корпуса компоненты частично или полностью погружены в диэлектрическую жидкость. При частичном погружении хладагент сначала доставляется к основным компонентам (процессорам, ускорителям и модулям памяти). Затем жидкость перетекает на серверную плату для охлаждения другой маломощной электроники. Ключевая особенность всех систем с по-

грузным шасси – возможность их интеграции в стандартные вертикальные стойки, часть которых может охлаждаться типовыми системами воздушного охлаждения.

Погружение в ванну (однофазное). ИТ-системы погружены в резервуар с диэлектрическим хладагентом, который находится в состоянии принудительной либо естественной конвекции, когда более теплая жидкость поднимается вверх. Охлаждение основано на способности жидкости поглощать тепловую энергию, зависящей от того, насколько хорошо хладагент рассеивает тепло и как быстро он обтекает охлаждаемые компоненты. Большинство производителей иммерсионных систем выбирают однофазный хладагент в силу его доступности, незначительного влияния на глобальное потепление, низкой стоимости и простоты внедрения.

Погружение в ванну (двухфазное). Серверы погружены в герметичный резервуар, заполненный диэлектрическим хладагентом, который кипит при относительно низкой температуре (например, 49°C) и при атмосферном давлении. Испаряясь, охлаждающая жидкость поглощает тепло ИТ-компонентов и как пар поднимается в конденсатор в верхней части резервуара, где конденсируется в жидкость и рециркулирует. Эксперты Uptime считают этот тип системы охлаждения наиболее подходящим для крупномасштабного использования, поскольку он обеспечивает высокую эффективность охлаждения, полностью поглощая тепловую нагрузку. Недостатки – проблемы с совместимостью материалов, высокая стоимость диэлектрической жидкости и ее потери из-за утечек.

В Uptime считают, что методы прямого жидкостного охлаждения будут совершенствоваться по мере удовлетворения требований клиентов и решения технических задач благодаря инновациям, стирающим границы между описанными выше подходами.

Экономическая выгода использования DLC не всегда очевидна. Способность жидкости отводить тепло намного выше, чем у воздуха, однако прямое жидкостное охлаждение применяется в очень немногих ЦОДах. Рассмотрим основные аргументы за и против DLC.

Стимулы и преимущества

Самый распространенный аргумент в пользу DLC, который приводят сегодня те, кто использует прямое жидкостное охлаждение, – необходимость поддерживать работу стоек высокой плотности. Но со временем станут важны и другие факторы. Четыре из них описаны ниже в порядке актуальности: от тех, с которыми придется считаться совсем скоро, до более отдаленных во времени.

Распространение высокопроизводительных приложений

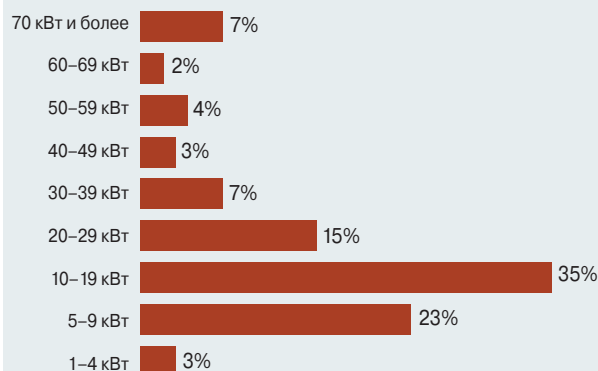
Высокопроизводительные приложения и системы высокой плотности, которые их обслуживают, используются все чаще. Более трети предприятий, принявших участие в нашем опросе, уже имеют ИТ-стойки мощностью более 20 кВт, почти каждое четвертое – мощностью более 30 кВт, а в каждом десятом работают несколько стоек мощностью более 60 кВт (рис. 1). И респонденты нашего опроса ожидают, что в будущем пиковая мощность их стоек возрастет. Примеры высокопроизводительных приложений: аналитика в реальном времени; транскодирование мультимедиа; облачные игры; инженерное моделирование; обучение сложных моделей искусственного интеллекта/машинное обучение на больших данных.

Охлаждение серверных чипов нового поколения

Серверные процессоры (ЦПУ и ускорители разных типов) будут потреблять все больше энергии и рассеивать все больше тепла. С каждым следующим технологическим поколением электронные цепи становятся все компактнее и мощнее. Поэтому увеличение плотности теплового потока (мощности на единицу площади) неизбежно. В предыдущее десятилетие ЦОДы уже столкнулись с тем, что типичная расчетная тепловая мощность процессора выросла примерно со 100 до 200 Вт, а в 2020-х мы ожидаем усиления этой тенденции: трех- или даже четырехкратного увеличения до более чем 600 Вт.

Отчасти из-за роста потребляемой мощности, отчасти из-за интеграции микросхем памяти в корпус процессора с более низкими пределами рабочих температур для чипов следующих поколений максимальная допустимая температура, измеренная на корпусе процессора, будет значительно ниже, что создаст дополнительную проблему для охлаждения серверов.

Какова максимальная мощность серверных стоек в ваших ЦОДах? (n = 162)



◀ Рис. 1. Распределение максимальной мощности серверных стоек в ЦОДах

Источник: Uptime Institute Intelligence

Информация, собранная Uptime, показывает, что все больше серверных продуктов будут иметь пониженные максимальные рабочие температуры, иногда до 55–60°C. Это намного ниже текущей нормы 70–90°C.

Первые высокопроизводительные и низкотемпературные серверные процессоры, скорее всего, появятся во второй половине 2022 г. Хотя поначалу они будут редкостью и будут использоваться в основном в суперкомпьютерах, мы ожидаем, что чипы такой конструкции станут обычным явлением во многих ЦОДах уже ко второй половине нынешнего десятилетия. Кроме того, с экономической точки зрения серверы, способные нести большую полезную нагрузку, предпочтительнее. В сочетании с необходимостью повышения производительности для отдельных бизнес- и технических приложений это создаст массовый спрос на такие процессоры со сложными тепловыми характеристиками. Дата-центры, которые не смогут работать с системами следующего поколения из-за их требований к охлаждению, поставят под угрозу свою конкурентоспособность по сравнению с организациями, которые обеспечат их поддержку.

Экологическая устойчивость

Общепринятые лучшие практики работы с воздушным охлаждением в ЦОДах оставляют мало возможностей для еще более эффективного использования энергии и воды. DLC предлагает снижение энергопотребления и одновременно почти полностью устраняет потребность в воде для охлаждения. Однако это не происходит автоматически и зависит от вариантов реализации и климатических условий на объекте.

Широкомасштабное внедрение DLC может также повысить экологическую устойчивость дата-центров, открывая возможности для реализации новых схем повторного использования тепла. Без более широкого внедрения DLC об-

щие показатели экологической устойчивости ЦОДов через несколько лет могут даже ухудшиться. Для некоторых будущих высокоплотных ИТ-систем рекомендуемая температура приточного воздуха будет снижена, что не позволит рассчитывать на системы охлаждения без чиллеров. Рекомендации ASHRAE по тепловому режиму в средах с оборудованием для обработки данных от 2021 г. не оставляют сомнений на этот счет.

Операционные расходы и капитальные затраты

Для многих предприятий, рассматривающих возможность перехода на DLC, главный аргумент – высокий потенциал повышения энергоэффективности. Частичный коэффициент энергоэффективности pPUE для систем прямого жидкостного охлаждения может составлять 1,02–1,03 при работе на повышенных температурах охлаждающей жидкости. DLC также экономит энергию благодаря отказу от вентиляторов в ИТ-системах и уменьшению потерь из-за статического электричества в кристаллах микросхем.

У DLC есть большой потенциал и для снижения капитальных затрат. Типичный ЦОД с воздушным охлаждением расходует приблизительно 25–35% общей мощности на обеспечение пиковой мощности и охлаждение. Эта мощность также должна поддерживаться генераторными установками, что требует больших капитальных и эксплуатационных затрат. Резерв мощности может быть существенно меньше, если на объекте используется в основном DLC. А в случае повышения ИТ-потребностей высвобождение резервов энергии вследствие перехода на жидкостное охлаждение поможет отсрочить капитальные вложения в уже эксплуатирующийся ЦОД или даже избежать их.

Наш опрос показал, что для предприятий, еще не использующих DLC, важнейшие аргументы перехода на прямое жидкостное охлаждение – экономия средств за счет снижения энергопотребления и повышение экологичности (рис. 2). По важности они опережают потребность в охлаждении ИТ-стоек с высокой плотностью размещения. Потенциальная экономия за счет уменьшения физической площади инфраструктуры – также важный довод в пользу DLC.

Барьеры и препятствия

Основная причина ограниченного распространения прямого жидкостного охлаждения – отсутствие стандартов для этой технологии. Работы в этом направлении ведутся, прежде всего в рамках Open Compute Project, но потребуются годы, чтобы они принесли плоды. И даже после утверждения стандарты повлияют лишь на часть

Рис. 2. Стимулы перехода на DLC



рынка. Пока же стандартов нет, при развертывании систем DLC возникает целый ряд проблем.

Совместимость материалов

Все компоненты, контактирующие с охлаждающей жидкостью, будь то очищенная вода, водно-гликолевые смеси или технические жидкости, должны быть тщательно проверены на совместимость. Сегодня блоки распределения охлаждающей жидкости (CDU) подходят только к конкретным системам DLC, и поэтому ЦОДы часто оказываются привязаны к одному или нескольким поставщикам. Совместимость особенно важна для иммерсионных систем, в которых ИТ-платы погружаются в жидкость и любое отклонение от заданных параметров может привести к неожиданным последствиям.

Несмотря на простоту, тщательное тестирование множества доступных комбинаций может потребовать значительного времени (часто – месяцев), организационных ресурсов и денег. Некоторые проблемы совместимости материалов проявляются не в виде явных отказов компонентов, а в виде неустойчивой работы, к примеру, падения производительности из-за потери целостности сигнала.

Поддержка ИТ-оборудования

Вендоры ИТ-оборудования не обеспечивают столь же полной поддержки систем жидкостного охлаждения, как воздушного. Иногда поставщики серверов предлагают системы DLC, интегрированные с ИТ-оборудованием, но обычно с очень узким выбором вариантов аппаратного обеспечения. Системы DLC третьих производителей поддерживаются, как правило, в индиви-

дуальном порядке. Если заказчик или его партнер-поставщик осуществляют интеграцию без явного согласия производителя ИТ-оборудования, гарантия на оборудование аннулируется.

Однако ситуация начинает меняться. Сформировалась небольшая, но растущая сеть партнерств между крупными поставщиками ИТ-оборудования и поставщиками систем DLC. Некоторые крупные системные интеграторы в настоящее время предлагают гарантии на ИТ-оборудование для более широкого спектра систем DLC, чем его производители.

Техническое обслуживание и эксплуатация

Для работы с системами DLC требуется переподготовка персонала. Кроме того, необходимо обновить процедуры технического обслуживания и эксплуатации для сотрудников, отвечающих и за инженерные, и за ИТ-системы. Обязанности по обслуживанию и эксплуатации систем прямого жидкостного охлаждения должны быть четко разделены. Важно определить, кто отвечает за блоки CDU – инженерная или ИТ-команда, а также установить регламент обслуживания ИТ-оборудования, охлаждаемого DLC-системой. Риски здесь повышаются из-за возможной утечки воды или диэлектрической жидкости.

Работа с системами на базе охлаждающих пластин не вызывает затруднений у опытных сотрудников, а вот погружение для большинства персонала ЦОДов процесс необычный, особенно если это погружение в резервуары с кипящими хладагентами. Переобучение персонала требует времени и денег, хотя это ценная инвестиция. Но даже при обученном персонале внедрение современных систем DLC повышает эксплуатацион-

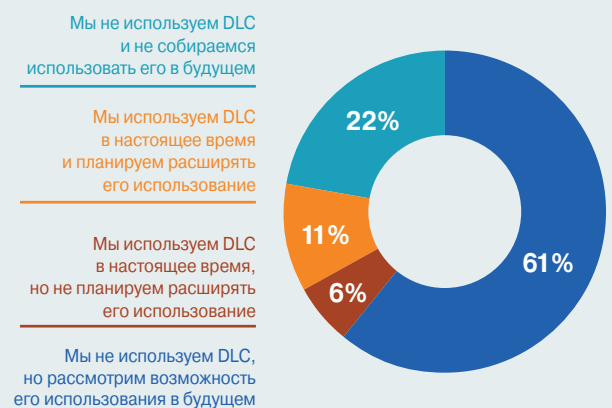
Какие из перечисленных проблем вы считаете основными препятствиями при развертывании DLC для собственных ЦОДов? Выберите не более трех (n = 104)



Источник: Uptime Institute Intelligence

▲ Рис. 3. Основные препятствия к внедрению DLC

Используете ли вы в настоящее время или планируете использовать какую-либо технологию DLC в собственных ЦОДах? (n = 179)



Источник: Uptime Institute Intelligence

▲ Рис. 4. Использование DLC сегодня и в будущем

ные риски из-за относительно низкой зрелости процедур и может привести к более высокому, чем обычно, числу сбоев и неполадок.

Первоначальная стоимость внедрения

Все вышеупомянутые факторы могут означать значительные затраты. Стоимость масштабного развертывания систем DLC увеличивают также расходы на сборку ИТ-систем на заказ и дополнительное оборудование охлаждения (блоки CDU, трубопроводы, новые стойки, а в случае иммерсионных систем – резервуары и диэлектрические жидкости, весьма дорогие для двухфазных систем). Стоимость внедрения чаще всего называется операторами ЦОДов главным препятствием перехода на жидкостные системы охлаждения, опережая опасения относительно утечек (рис. 3). Эти затраты могут быть компенсированы при строительстве нового дата-центра или при наращивании мощностей за счет экономии на капиталовложениях в инфраструктуру воздушного охлаждения, в недвижимость и/или за счет уплотнения ИТ-оборудования.

DLC сегодня и через пять лет

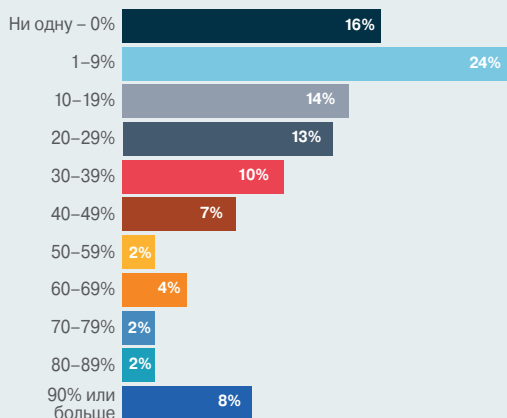
Из принявших участие в нашем опросе почти 200 операторов корпоративных ЦОДов примерно каждый шестой в настоящее время использует прямое жидкостное охлаждение (рис. 4). Почти две трети респондентов заявили, что намерены рассмотреть возможность применения DLC в своей инфраструктуре. Пятая часть не готова к использованию DLC по разным причинам – от отсутствия ожидаемой потребности в высокоплотных ИТ-мощностях и достаточной производительности существующих систем воздушного охлаждения до нежелания подводить к серверам трубы с водой.

Отвечая на вопрос о возможном использовании DLC в течение пяти ближайших лет, большинство респондентов прогнозируют, что по крайней мере 10% их стоек будут оснащены прямым жидкостным охлаждением, и лишь каждый шестой не ожидает появления в своих ЦОДах стоек с DLC. Выделяется также небольшая группа с повышенными амбициями: каждый десятый прогнозирует, что их ИТ-инфраструктура практически полностью перейдет на жидкостное охлаждение в течение пяти лет (рис. 5).

Самый популярный тип DLC, возможность внедрения которого рассматривают предприятия, – это охлаждающие пластины с водой или водно-гликолевыми жидкостями. Это объясняется, по всей вероятности, тем, что такие системы широко доступны и наиболее понятны в эксплуатации (рис. 6). Вторым наиболее подходящим вариантом считаются охлаждающие пластины с диэлектрическими хладагентами, хотя они появились относительно недавно. Иммерсионные системы выбрало небольшое количество участников опроса, что можно объяснить масштабами изменений, которые повлечет их внедрение в проекты ЦОДов, цепочки поставок и эксплуатацию.

При этом более трети респондентов заявили, что не знают, какую конкретно технологию DLC будет рассматривать их предприятие. Эта неопределенность может отражать отсутствие ясности в характеристиках разных платформ из-за малого количества внедрений, что не позволяет предприятиям сформировать более четкое представление о них. У экспертов Uptime сложилось схожее мнение о рынке DLC, который все еще находится в движении: потенциальные клиенты ЦОДов изучают варианты, запускают

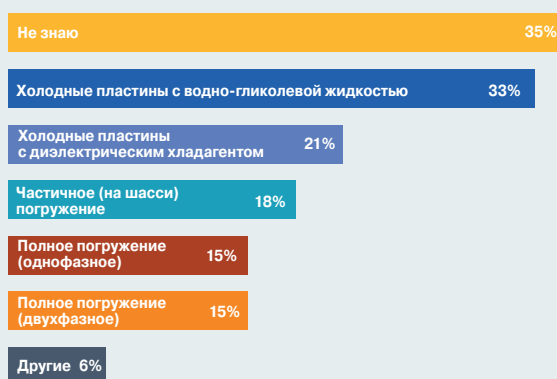
Какой процент ваших ИТ-стоек в течение ближайших трех-пяти лет вы планируете оснастить DLC (если планируете)? (n = 119)



Источник: Uptime Institute Intelligence

▲ Рис. 5. Ожидаемая доля ИТ-стоек с DLC в течение пяти лет

Какие типы DLC ваша организация рассматривает для установки в корпоративных ЦОДах? Выберите все подходящие (n = 110)



Источник: Uptime Institute Intelligence

▲ Рис. 6. Популярность различных систем DLC



пилотные проекты и тестируют системы прямого жидкостного охлаждения для сбора данных и накопления опыта эксплуатации.

Подведем итоги

Прямое жидкостное охлаждение всегда использовалось в охлаждении ИТ-инфраструктуры, но почти исключительно в мейнфреймах и суперкомпьютерах. Было реализовано несколько проектов DLC для ИТ-инфраструктуры общего назначения, но пока это лишь исключение из правила – воздушного охлаждения.

Согласно данным, проанализированным Uptime, сфера применения DLC будет расширяться, поскольку тепловая мощность высокопроизводительных серверных микросхем растет, а их предельные рабочие температуры снижаются. Воздушное охлаждение не сможет работать с этими чипами без серьезных компромиссов, таких как более крупные радиаторы и более высокая мощность вентиляторов, или (что еще хуже) без необходимости снижения температуры воздуха. Темпы внедрения DLC в ЦОДах будут в значительной степени определяться спросом на повышение производительности приложений и эффективности инфраструктуры при внедрении процессоров следующего поколения.

Тем не менее, чтобы изменить архитектуру охлаждения в ЦОДах, не нужен полный или массовый переход на DLC. Даже относительно небольшое количество ИТ-систем, для которых необходимо прямое жидкостное охлаждение, может изменить требования к объекту, если ожидается, что они будут работать в сочетании с системами воздушного охлаждения, как в случае с охлаждающими пластинами и системами с погружным шасси. Например, понадобится поддержка блоков CDU на уровне всего дата-центра. А наличие лишь нескольких систем с погружением в ванну потребует выделенной зоны и дополнительного пространства для обслуживания ИТ-оборудования.

Неопределенность перспектив внедрения DLC усложняет планирование мощности подводимо-

го электропитания. С одной стороны, операторы ЦОДов не хотят слишком быстро исчерпать ресурсы и получить пустоту в машинных залах, с другой – не хотят переплачивать за мощность, которая никогда не будет востребована.

Похоже, что прямое жидкостное охлаждение теперь заинтересует не только тех, кто эксплуатирует высокоплотные ИТ-стойки, но и гораздо более широкую категорию заказчиков, имеющую всего несколько серверов с высокопроизводительными/низкотемпературными компонентами наряду со стандартным ИТ-оборудованием, которое, вероятно, останется на воздушном охлаждении.

Несмотря на то что распространение DLC точно смоделировать невозможно, эксперты Uptime видят убедительные доказательства общего движения в этом направлении. Растущий спрос на вычислительные ресурсы в сочетании со стремлением снизить затраты на ЦОДы и увеличить экологическую устойчивость также стимулирует внедрение DLC. Однако это внедрение, вероятно, будет сдерживаться раздробленностью рынка поставщиков, недостатком компонентов, организационной инерцией и отсутствием формальных стандартов.

Весьма вероятно, что в ближайшие несколько лет один-два крупных оператора ЦОДов примут стратегические решения использовать DLC в стандартных проектах своих дата-центров следующего поколения. Это может подтолкнуть участников более широкой экосистемы производителей систем охлаждения ЦОДов и ИТ-оборудования увеличить инвестиции в разработку продуктов DLC и их крупносерийное производство, что, в свою очередь, может привести к стандартизации де-факто одного или двух типов технологии прямого жидкостного охлаждения.

Тренды микропроцессорных технологий в сочетании с потребностями бизнеса в повышении производительности и экологичности инфраструктуры указывают на то, что широкое распространение DLC – лишь вопрос времени. **ИКС**

Трансформация бизнеса, трансформация продуктового предложения

Образованная в результате продажи бизнеса Schneider Electric в РФ и Беларуси локальному руководству компания Systeme Electric сегодня имеет один из самых полных портфелей решений для ЦОДов. Подробнее – Алексей Соловьев, технический директор управления по рынку «Информационные технологии».



– Какие продукты Systeme Electric предлагает для инженерной инфраструктуры ЦОДов?

– Прежде чем ответить на этот вопрос, напомним, что предлагала рынку компания Schneider Electric: основной фокус был сделан на создании комплексной инженерной инфраструктуры, которая включала в себя все основные и критически важные элементы, – другими словами, моновендорного решения. Это было одним из ключевых преимуществ, мы первые представили такой подход, и рынок положительно оценил достоинства экосистемы.

Сейчас, в процессе трансформации нашего бизнеса, продуктового предложения, мы сохраняем нацеленность на эту комплексность и активно выводим на рынок новые решения в тех же продуктовых направлениях, что и раньше.

В первую очередь речь идет о распределении электропитания в ЦОДе: начиная от ввода и далее, через оборудование распределения, шин, проводы, бесперебойное электропитание и заканчивая стоечными PDU в серверных шкафах. Для системы охлаждения – это чиллерные установки и кондиционеры воздуха в машинных залах. Система размещения ИТ-оборудования представлена разными линейками серверных шкафов и системами изоляции воздушных потоков. Все это планируется объединить под контролем единой централизованной системы мониторинга и управления инженерной инфраструктурой и жизненным циклом ЦОДа, а также поддерживать с помощью различных сервисных услуг. Здесь важно отметить, что команда, занимающаяся развитием продукта в стране, осталась прежней, а значит, осталось понимание потребностей рынка и того, как воплотить их в продукте.

– Полон ли портфель продуктов настолько же, насколько был у ушедшей с рынка Schneider Electric?

– Мы ставим себе задачу в течение этого и следующего года наполнить портфель продуктами во всех целевых направлениях и предложить рынку те самые всеобъемлющие решения. Естественно,

мы не собираемся ждать последнего элемента этой структуры, а выводим продукты по мере их готовности. Например, мы уже представили новые трехфазные ИБП серии Uniprom мощностью от 10 до 600 кВт и серию серверных шкафов серии Uniprom Rack с блоками Uniprom PDU. Немаловажный аспект – новые продукты производятся на тех же производственных мощностях, что и продукты Schneider Electric, т.е. мы можем опираться на политики стандартов качества и культуры производства. Уже доступны к заказу периметральные и внутрирядные кондиционеры CoolRoom и CoolRow, а также чиллеры CoolFlow. Дальше в наших планах не только расширять продуктовую линейку, но и фокусироваться на «частных случаях» продуктов для узкоспециализированных задач наших заказчиков. В итоге портфель продуктов будет полным, но при этом в нем будут учтены специфика и требования именно нашего, а не глобального рынка.

– Поскольку Systeme Electric готовит продукты именно для российского рынка (в отличие от глобальных предложений Schneider Electric), они должны быть лучше адаптированы к потребностям наших заказчиков. В чем это проявляется?

– Да, у нас появилась возможность более оперативно влиять на технические функции продукта и учитывать требования отдельных заказчиков. Например, добавлять функционал, если он необходим, или избавляться от него, если он избыточен и влияет на цену. Если раньше вопросы коинжиниринга обсуждались в основном для проектов ЦОДов формата XL и выше, то сейчас такой планки нет, как нет и ограничений по типу продуктов, в которые можно вносить изменения. Например, в ходе обсуждения вопросов размещения ИТ-оборудования в одном из проектов мы поняли, что количество розеток в стандартных блоках распределения питания меньше количества устанавливаем-

мого в шкаф оборудования. Это можно было бы исправить за счет добавления второго БРП, однако мы сделали по-другому – изменили конструкцию БРП и добавили эти недостающие розетки. В итоге в шкафу осталось дополнительное место для организации кабелей, и это не сильно отразилось на общей стоимости шкафа.

Отдельно отмечу, что Systeme Electric – это российская производственная компания, и мы активно работаем над локализацией производства на наших предприятиях внутри страны. Часть оборудования уже выпускается на территории России, и мы планируем максимально использовать наши производственные мощности для локализации как можно большего ассортимента продукции.

– В чем основные конкурентные преимущества Systeme Electric?

– Когда речь заходит о преимуществах, многие начинают сравнивать технические детали отдельных продуктов. Однако далеко не всё можно вложить в базовые метрики. Помимо технических характеристик каждый продукт обладает еще набором дополнительных преимуществ, в которые мы также инвестируем.

Во-первых, у нас есть глубокая экспертиза как в продуктах, так и в технологиях. Эта экспертиза была создана Schneider Electric, и нам удалось ее сохранить.

Во-вторых, это сервисная и техническая поддержка. После покупки наступает длительный период эксплуатации. Это редко учитывают в техническом сравнении, обычно ограничиваются коротким «это есть», однако качество и доступность того, «что есть», различается. Это сильно влияет на оценку рисков, с которыми сталкивается эксплуатирующая сторона, особенно если речь идет о критической инфраструктуре ЦОДа или предприятия. Мы уделяли этому большое внимание раньше и не собираемся отказываться от этого преимущества в новой компании.

В-третьих, мы выстраиваем наш бизнес и наше продуктивное предложение как экосистему, и такого предложения на рынке сегодня нет ни у кого. Экосистема строится по нескольким направлениям: на техническом уровне, когда продукты формируют инфраструктурное решение, охватывая все критические подсистемы, включая автоматизацию и управление; на уровне жизненного цикла ЦОДа, когда на всех этапах мы готовы помогать заказчикам экспертизой и сервисами, начиная с этапов планирования и проектирования, затем на этапах внедрения, эксплуатации и модернизации объекта; и на уровне бизнеса, обеспечивая взаимодействие на всех уровнях – вендор, дистрибуция, каналы продаж, заказчики, сервис и поддержка.

– Существует мнение, что российскому рынку ЦОДов не избежать технологической деградации. Что вы думаете на этот счет?

– С точки зрения присутствия тех или иных вендоров наш рынок в этом году сильно изменился, кто-то одновременно ушел, кто-то трансформировал бизнес, пришли новые, мало известные ранее бренды. Но при этом утверждать, что с этими изменениями драматически ухудшились технические характеристики продуктов, я не могу. С одной стороны, ни у кого не было монополии на ту или иную технологию, чтобы говорить о полном ее исчезновении без альтер-

натив. С другой стороны, новые появившиеся на рынке производители и поставщики, в основном китайские, делают ставку на завоевание доли рынка за счет снижения цены, которое достигается в том числе путем упрощения систем. В моменте это может дать ощущение того, что в среднем произошла деградация. Но при этом же существуют компании, которые инвестируют в технологии, понимая, что бесконечно упрощаться не получится. Поэтому думаю, что высокотехнологичный сегмент восстановится, пусть с изменениями в составе, что должно положительно сказаться и на средних по отрасли технических характеристиках.

Мы в Systeme Electric сохранили собственный R&D-центр и продолжим в него инвестировать. Помимо удовлетворения сегодняшних потребностей наших заказчиков мы работаем над тем, чтобы завтра предложить нашему развивающемуся рынку более технологичные решения. Это касается как внедрения технологий в «железо», так и развития программных продуктов. В Systeme Electric есть отдельный департамент, базирующийся в Иннополисе (Татарстан), который разрабатывает программные решения для автоматизации и управления ресурсами ЦОДа.

– Как в целом будет развиваться российский рынок цодостроения и какое место на нем планирует занять Systeme Electric?

– Российский рынок ЦОДов в последние годы показывал устойчивую положительную динамику по вводимым новым объектам. В ближайшей и среднесрочной перспективе эта динамика сохранится. Мы видим, что с рынка ушел ряд вендоров, но появляются новые игроки. И для заказчика становится крайне актуальным вопрос о стабильности компаний на рынке и готовности к долгосрочным инвестициям в этот рынок. Важно помнить, что основное инженерное оборудование в ЦОДе эксплуатируется не менее десятка лет, и в течение всех этих десяти с лишним лет оно должно иметь надежное сервисное обеспечение со стороны вендора. Systeme Electric продолжает исполнять все обязательства по поддержке оборудования Schneider Electric. Мы являемся единственным авторизованным сервисным партнером и за счет собственной сервисной службы поддерживаем инсталлированную базу Schneider Electric. Более того, при определенных условиях мы можем взять на обслуживание инсталлированную базу заказчика. Основная цель – не оставить заказчика один на один с оборудованием ушедших с рынка вендоров.

В результате трансформации из Schneider Electric в новую компанию Systeme Electric нам удалось сохранить основное: экспертизу, связь с рынком, наши производственные мощности, сервисную и техническую поддержку заказчиков – все то, что определяло нас как одного из лидеров отрасли. Трансформация продуктового предложения дает нам возможность предложить заказчикам новые решения, которые позволят реализовать стратегии развития их ИТ-инфраструктуры в новых условиях.

Архитектура Spine – Leaf в ЦОДах: зачем нужна и как реализовать

Андрей Семенов, профессор, МТУСИ

Применение архитектуры Spine – Leaf при построении локальной сети ЦОДа уменьшает задержку передачи сигнала между вычислительными узлами. Для повышения эксплуатационной гибкости и улучшения экономических характеристик целесообразно выбирать вариант с центральным кроссом.

Традиционная архитектура информационной системы ЦОДа и ее недостатки

Аппаратная часть информационной системы машинного зала ЦОДа – это комплекс компьютерного и сетевого оборудования, а также дополняющей его информационной проводки. Активная часть этого комплекса состоит из трех функциональных блоков:

- локальной вычислительной сети (ЛВС);
- сети системы хранения данных (массовой памяти) (СХД);
- совокупности серверов, которые, собственно, и обрабатывают информацию.

Многочисленные серверы этого комплекса представляют собой терминальное оборудование информационной инфраструктуры машзала ЦОДа. По разным направлениям они

взаимодействуют с ЛВС и СХД, находясь между ними.

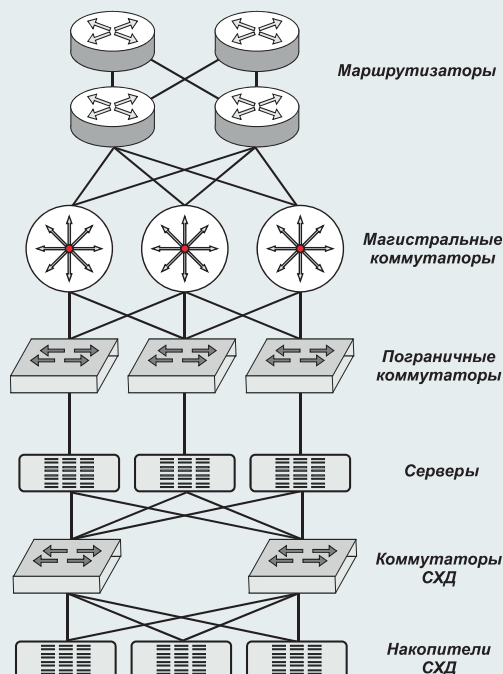
Физический уровень информационной инфраструктуры машзала ЦОДа реализуется согласно требованиям и рекомендациям американского стандарта ANSI/TIA-942A, его международного аналога ISO/IEC-11801-5 и отечественного стандарта ГОСТ Р 59486:2021. Информационная проводка выполняется в форме СКС, причем для ее создания безальтернативно применяется волоконная оптика. Медножильная элементная база в состоянии обеспечить скорость передачи данных не более 25–40 Гбит/с, что не соответствует современным требованиям (необходимо как минимум 100 Гбит/с). Поэтому электропроводные линии целесообразно использовать только для создания второстепенных внутрирядных соединений.

ЛВС и СХД обслуживают большое количество серверов, и строить их целесообразно по иерархическому принципу, чтобы полноценно воспользоваться теми преимуществами, которые дает мультиплексирование при переходе на более высокий уровень иерархии.

В общем случае в классической структуре выделяются верхние уровни ядра и следующего за ним уровня агрегации (распределения), которые дополнены уровнем доступа (рис. 1). Популярность такой схемы обусловлена эксплуатационной гибкостью, простотой формирования резервных связей и неплохими стоимостными показателями благодаря высокой связности отдельных серверов. Это позволяет не закладывать в систему избыточную пропускную способность каналов связи и использовать при формировании временных связей простейшие средства маршрутизации нижнего уровня.

Главный и принципиально неустранимый недостаток классической архитектуры – большое время задержки сигнала вследствие передачи сообщения через множество промежуточных узлов. Сегодня же очень важна малая задержка,

Рис. 1. Классическая схема информационной сети крупных ЦОДов ▶



поскольку ЦОДы зачастую обеспечивают работу приложений, для которых используются виртуализация и программное определение вычислительной структуры, из-за чего серверы вычислений и СХД могут располагаться в любых местах машзала.

Основная идея архитектуры Spine – Leaf

Значимого снижения времени задержки при существующем уровне техники можно добиться только уменьшением количества промежуточных узлов между произвольно взятой парой серверов. Это, в свою очередь, можно сделать, если свести количество уровней локальной сети машзала к двум.

Двухуровневая архитектура, называемая также децентрализованной ячеистой (mesh) архитектурой, обладает рядом достоинств, благодаря чему она получила широкое распространение и даже специальное наименование – Spine – Leaf. Ее идея предельно проста: в этой архитектуре каждый коммутатор нижнего уровня (Leaf) соединен выделенной неблокируемой связью с каждым коммутатором верхнего уровня (Spine). Основное достоинство архитектуры Spine – Leaf заключается в том, что при обмене данными между двумя произвольно взятыми серверами трафик проходит только через один коммутатор верхнего уровня Spine и задержка сигнала становится предсказуемой и согласованной.

Таким образом, выигрыш по ключевому параметру времени задержки достигается резким увеличением количества связей для обмена данными между отдельными узлами.

Spine – Leaf и структура информационной системы машзала ЦОДа

Архитектура Spine – Leaf практически идеально соответствует традиционной структуре информационной системы машзала ЦОДа.

Здесь, в отличие от офисных систем, данные передаются преимущественно между серверами (направление «восток – запад»), а не от терминального устройства пользователя-человека к серверу и обратно («север – юг»).

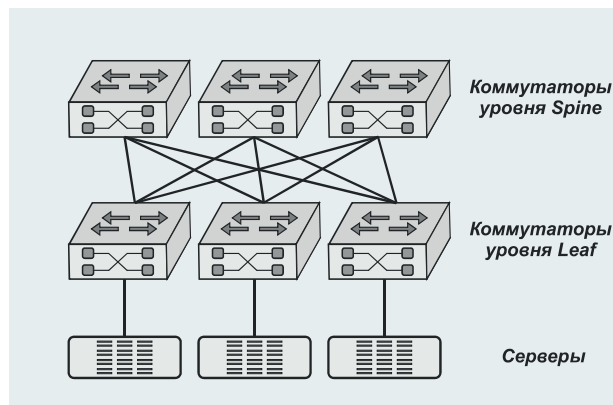
Структура Spine – Leaf без проблем создается также при построении ЛВС по популярной схеме Top of Rack (ToR). В этом случае увеличивается количество пограничных коммутаторов, которые устанавливаются непосредственно в серверный шкаф (или размещаются непосредственно над ним, что с системной точки зрения то же самое) и выполняют в дальнейшем функции коммутаторов уровня Leaf (рис. 2).

Пожалуй, наиболее серьезная особенность подобной переконфигурации сети состоит в том, что схема Top of Rack экономически привлекательна только при высокой степени утилизации портов пограничных коммутаторов. В момент запуска ЦОДа в эксплуатацию это условие выполняется далеко не всегда, и ресурсы, направленные на упреждающее развертывание дорогостоящего высокоскоростного сетевого оборудования, оказываются на длительное время заморожены. Ситуацию можно частично исправить объединением пограничных и магистральных коммутаторов в одном аппаратном шкафу. Тогда коммутация оборудования разных уровней осуществляется обычными аппаратными шнурами или активными кабельными сборками.

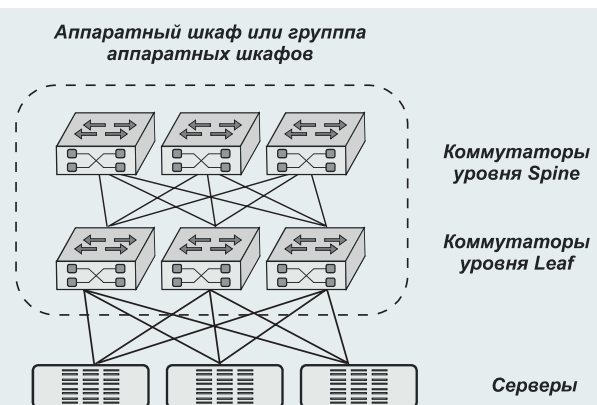
Немаловажное достоинство топологии с применением выделенных аппаратных шкафов (рис. 3) – простота разграничения прав доступа к оборудованию специалистов различных служб, что положительно сказывается на коэффициенте готовности объекта.

Особенности кабельной системы для поддержки архитектуры Spine – Leaf

Архитектура Spine – Leaf открыта на транспортном уровне. При необходимости нарастить



▲ Рис. 2. Построение нижнего уровня ЛВС машзала ЦОДа на основе архитектуры Spine – Leaf при установке пограничных коммутаторов по схеме Top of Rack



▲ Рис. 3. Построение нижнего уровня ЛВС машзала ЦОДа при реализации архитектуры Spine – Leaf с выносом коммутаторов в отдельный шкаф (группу шкафов)

производительность ЛВС машзала на уровнях Spine и Leaf в нее без проблем добавляются соответствующие коммутаторы.

В то же время рассматриваемая архитектура полностью совместима с созданными ранее и ставшими уже классическими решениями сетевых интерфейсов и кабельных трактов. Таким образом, новых разработок не требуется.

Физический уровень Spine – Leaf сложнее традиционной архитектуры в первую очередь в количественном смысле: требуется больше кабелей и точек коммутации, что затрудняет текущее администрирование. Тем не менее даже при жестких бюджетных ограничениях сравнительно высокие по сравнению с традиционными офисными сетями затраты на реализацию физического уровня несущественны с системной точки зрения, не говоря уже об их малости по сравнению с расходами на строительство или подготовку здания ЦОДа, реализацию электроснабжения, кондиционирования и иных инженерных систем.

Достижение эксплуатационной гибкости архитектуры Spine – Leaf

Единственный существенный недостаток физического уровня архитектуры Spine – Leaf в случае его реализации как СКС стандарта ISO/IEC 11801-5 – малая эксплуатационная гибкость: добавление новых коммутаторов в первую очередь нижнего уровня Leaf вне зависимости от выбранной топологии влечет за собой необходимость прокладки новых линий. В действующем ЦОДе это крайне нежелательно из-за высокого риска нарушения нормального кондиционирования машинного зала.

Устранить этот недостаток можно, модернизирував топологию кабельной системы, а именно, добавив вспомогательный главный кросс К, в который сводятся соединительные линии для подключения серверов и коммута-

торов нижнего уровня Leaf (рис. 4). Сами линии вместо упреждающей прокладки в процессе строительства ЦОДа вполне можно создавать по мере необходимости, что намного выгоднее с финансовой точки зрения.

Структура с дополнительным центральным кроссом сохраняет все преимущества модульно-кассетного подхода к реализации кабельных трактов. Транковые кабели и кассеты можно вводить в состав кабельной системы по мере необходимости. Это преимущество распространяется и на процесс изменения схемы передачи, что требуется при наращивании скорости информационного обмена и решается заменой кассет. Последние фактически выполняют функцию корпусного адаптера и позволяют перейти на новую схему реализации трактов передачи кабельной системы. Это весьма удобно с эксплуатационной точки зрения.

Архитектура на рис. 4 основана на формировании составных трактов на участке от любого из серверов до произвольного коммутатора Leaf. Они не могут быть реализованы на стандартной элементной базе из-за превышения допустимого бюджета потерь для нормальной работы основной массы высокоскоростного сетевого оборудования. Данная проблема, однако, легко решается использованием более качественных разъемов класса Elite или их аналогов.

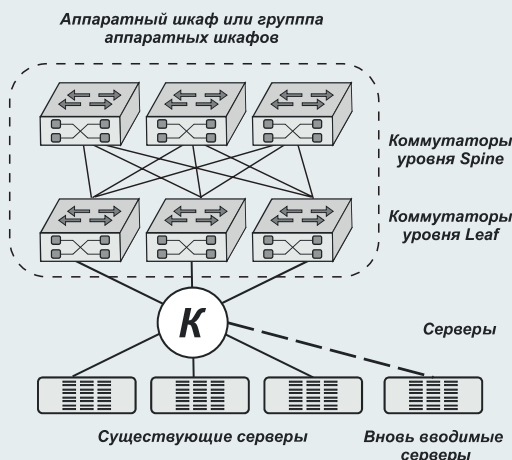
■ ■ ■

Архитектура Spine – Leaf – продукт естественного развития классических подходов к построению физического и транспортного уровня информационной инфраструктуры ЦОДа. Благодаря существенному снижению задержки передачи сигнала она имеет широкие перспективы практического применения при условии использования на физическом уровне сети волоконной оптики. Причем реализовать архитектуру Spine – Leaf можно на известной элементной базе, новых разработок не требуется.

Модернизация на физическом уровне сводится к установке дополнительного центрального кросса, наличие которого значительно увеличивает эксплуатационную гибкость физического уровня информационной инфраструктуры машзала ЦОДа. Двойное сокращение средней длины кабелей сборки несколько упрощает развертывание линейной части информационной проводки.

Главный недостаток архитектуры Spine – Leaf – удвоение количества оптических претерминированных сборок на физическом уровне. Поэтому ее применение ужесточает требования к планированию кабельных трасс с учетом перспектив развития ЦОДа. ИКС

Рис. 4. Построение нижнего уровня ЛВС машзала при реализации архитектуры Spine – Leaf с дополнительным главным кроссом (К) ▶



Wi-Fi на 6 ГГц. Куда все идет?

Количество устройств, подключенных к сетям Wi-Fi, постоянно растет, и соответственно растет потребность в повышении скорости и емкости этих сетей. Выделенный для них новый диапазон призван удовлетворить эти запросы.

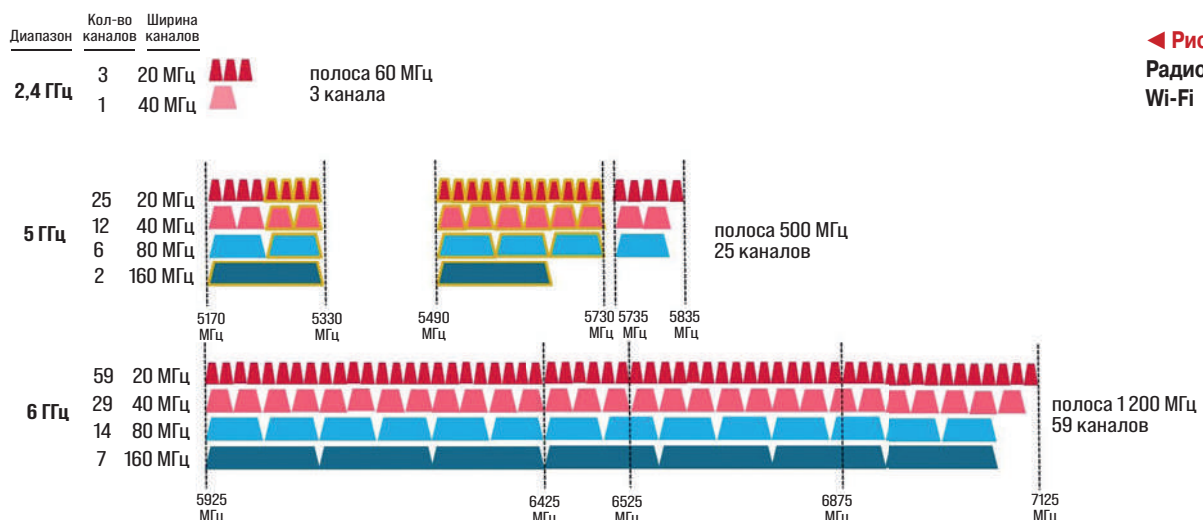
Предпосылки возникновения стандарта Wi-Fi 6E

За прошедшее десятилетие количество пользователей, подключенных к беспроводным сетям, увеличилось минимум вдвое, и объем данных, передаваемых через них, непрерывно растет. Квартиры оснащаются системами «умный дом», а бесплатные сети Wi-Fi появились не только в транспорте, гостиницах и кафе, но и во многих открытых общественных пространствах. Один из факторов, влияющих на рост трафика, – передача и просмотр видео. Недавно одна иностранная компания опубликовала съемки затонувшего «Титаника» уже в качестве 8К. Для беспере-

бойного воспроизведения такого видеоматериала нужна хорошая пропускная способность сети. Поэтому неудивительно, что некоммерческий альянс Wi-Fi Alliance принял решение выпустить расширенную версию стандарта Wi-Fi 6 – Wi-Fi 6E (Extended), которая в теории может обеспечить передачу данных со скоростью до 9,6 Гбит/с и способна работать в новом частотном диапазоне 6 ГГц.

Предполагалось, что стандарт Wi-Fi 6 (802.11ax) должен ускорить цифровизацию на предприятиях, обеспечить автоматизацию процессов производства, развитие интернета вещей (IoT), создание облачных решений и т.д.

Никита Куликов,
сетевой архитектор
направления
сетевых решений,
«ЛАНИТ-Интеграция»
(ГК ЛАНИТ)



◀ **Рис. 1.**
Радиоканалы
Wi-Fi

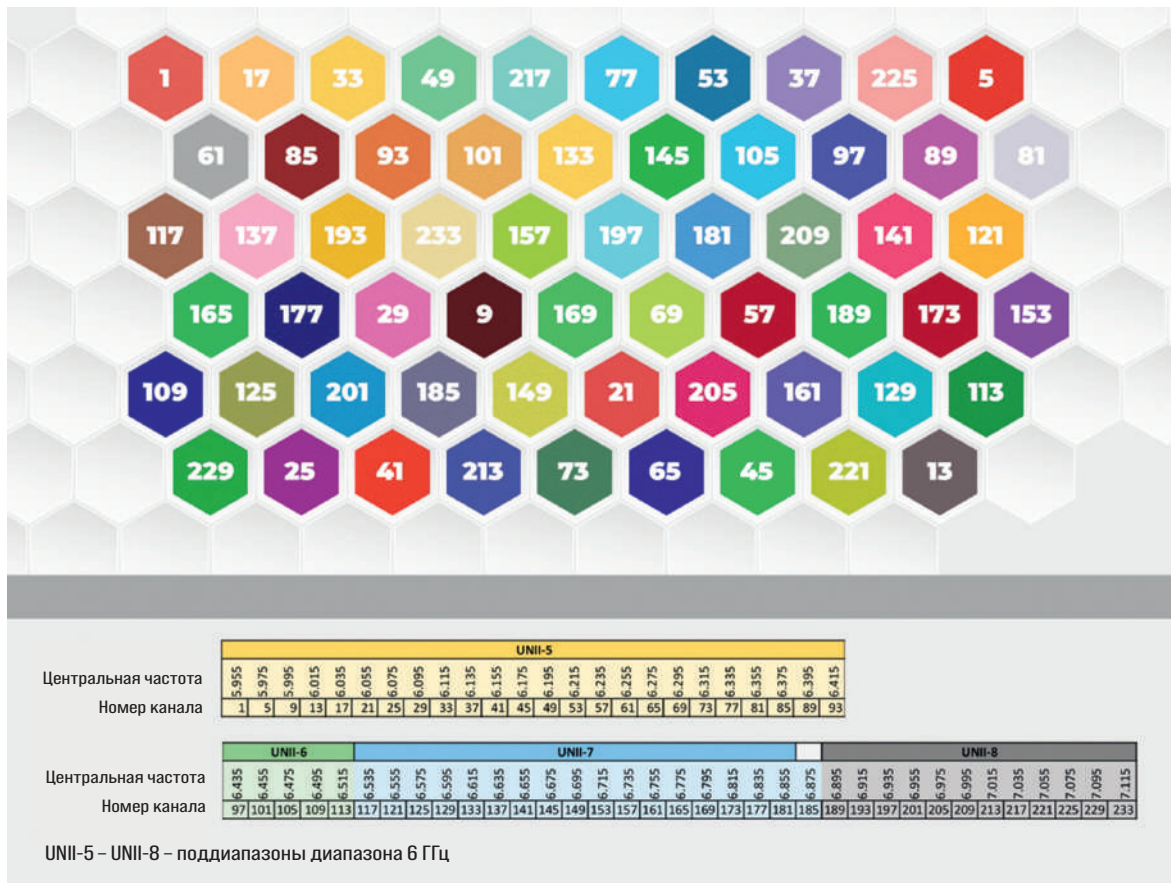


Рис. 2. Пример распределения каналов диапазона 6 ГГц

Основные отличия Wi-Fi 6 от предыдущего пятого поколения – более высокая скорость передачи данных и использование технологии OFDMA (множественный доступ с ортогональным частотным разделением каналов). В такой сети увеличится количество пользователей, которые смогут одновременно подключаться не только безопасно, но и без потери скорости.

Отличие же Wi-Fi 6E от Wi-Fi 6 в том, что устройства этого стандарта будут способны работать и в частотном диапазоне 6 ГГц, в котором устройства предыдущих стандартов, включая Wi-Fi 6, работать не будут и, следовательно, не будут создавать помехи. Благодаря этому пользователь сможет передать огромный массив данных за минимальное время. Устройства, которые поддерживают Wi-Fi 6E, уже существуют: это Asus Zenfone 9, Motorola Moto S30 Pro и некоторые модели ноутбуков.

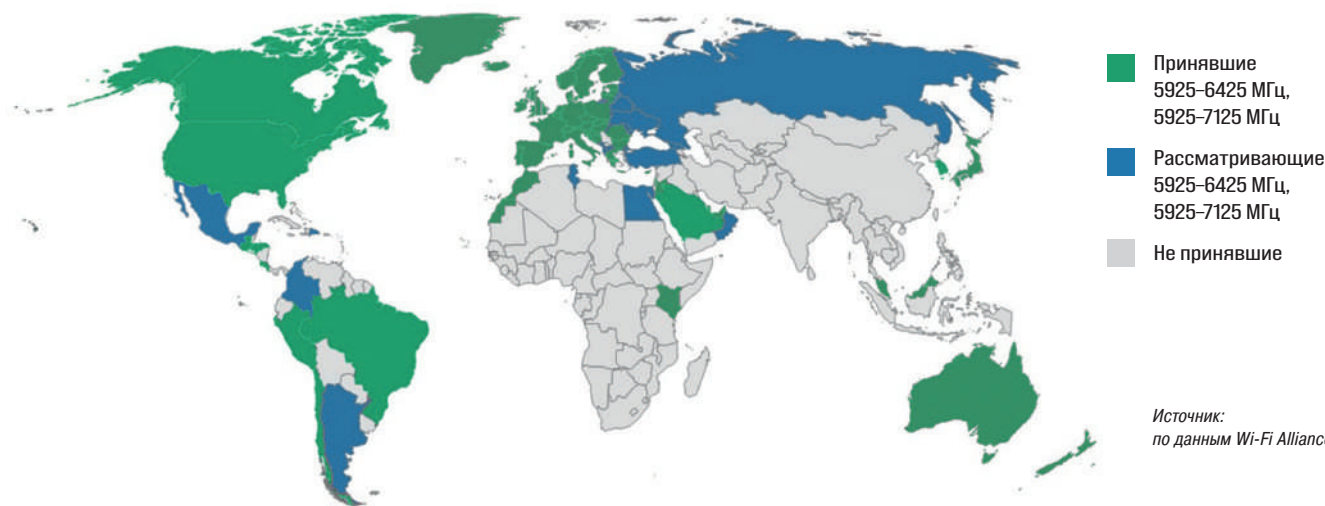
Преимущества использования диапазона 6 ГГц в Wi-Fi

Наряду с ростом количества устройств, работающих в сетях Wi-Fi, растет и загрузка используемых ими каналов, что снижает скорость передачи и получения данных. Поэтому для стандарта Wi-Fi 6E дополнительно выделен частотный диапазон 5925–7125 МГц шириной 1200 МГц. Это дает возможность при проектировании Wi-Fi-сетей использовать 59 но-

вых радиочастотных каналов шириной 20 МГц. Прежде было доступно всего 28 таких каналов: три – в диапазоне 2,4 ГГц и 25 – в диапазоне 5 ГГц (рис. 1). Таким образом, количество доступных каналов увеличилось более чем втрое. В новом диапазоне достигается компромисс между количеством используемых частот и дальностью распространения радиосигнала Wi-Fi, которая уменьшается при повышении частоты.

Выделяют два основных преимущества использования Wi-Fi 6E.

Увеличение пропускной способности каналов связи. Клиентские устройства с каждым годом становятся мощнее и требовательнее к пропускной способности сетей доступа Wi-Fi, которая напрямую зависит от ширины канала связи. Поскольку новый диапазон непрерывный, его можно разбить на семь непересекающихся каналов шириной 160 МГц. В предыдущем стандарте было доступно лишь два канала такой ширины в диапазоне 5 ГГц. При подобных условиях построить сеть Wi-Fi с каналами шириной 160 МГц было физически нельзя. С выходом же Wi-Fi 6E такая возможность появилась. Теперь, имея девять непересекающихся каналов 160 МГц, можно построить беспроводную сеть с более высокой пропускной способностью. Такие сети Wi-Fi необходимы, скажем, службам потокового вещания видео, которым нужно высокое качество при воспроизведении медиа-



контента, и сервисам дополненной и виртуальной реальности (AR/VR).

Уменьшение задержек. Наличие большого количества новых каналов позволяет практически избавиться от интерференции радиоволн, когда соседние устройства работают на одних и тех же или соседних частотах. Это, в свою очередь, снижает задержки при передаче данных. Благодаря новому диапазону можно покрыть сеть Wi-Fi площадь около 20 000 кв. м без повторного использования каналов (рис. 2). Такая беспроводная сеть вполне пригодна, например, для гостиниц и больниц, где практически в каждой комнате устанавливаются отдельные точки доступа.

Однако работать в новом диапазоне 6 ГГц смогут только устройства, поддерживающие Wi-Fi 6E. Это исключает проблемы обратной совместимости, когда в канале одновременно работают устройства старых и новых стандартов, и позволит полностью раскрыться потенциалу Wi-Fi 6E.

В то же время у диапазона 6 ГГц есть ряд недостатков.

- Повышенное затухание сигнала беспроводной сети по сравнению с диапазонами 5 и 2,4 ГГц. Чем выше частота радиосигнала, тем он быстрее ослабевает в пространстве. Соответственно, при построении сетей Wi-Fi 6E важно учитывать, что плотность точек доступа должна быть выше.
- Более высокая стоимость одной точки доступа Wi-Fi. Дело в том, что в ней необходимо устанавливать дополнительный радиомодуль для работы в диапазоне 6 ГГц, что увеличивает конечную стоимость устройства.
- Дополнительный радиомодуль увеличит общее энергопотребление точки доступа. Для питания точек доступа понадобятся коммутаторы с поддержкой технологии Power over

Ethernet стандарта не ниже 802.3at (PoE+), а если потребуется работа всего функционала, то 802.3bt (PoE++). Также порты подключения точек доступа на коммутаторах должны будут поддерживать MultiGigabit Ethernet 802.3bz (2,5 и 5 Гбит/с), поскольку с появлением дополнительного модуля пропускная способность увеличится и просто гигабитного подключения будет уже недостаточно.

Все это в совокупности увеличит стоимость построения беспроводных сетей с поддержкой Wi-Fi 6E.

Использование диапазона 6 ГГц для Wi-Fi в мире и в России

По данным Wi-Fi Alliance, 27 стран уже приняли решение об использовании диапазона 6 ГГц для работы сетей Wi-Fi, а еще в 14 странах этот вопрос находится в стадии рассмотрения (рис. 3).

Распространение оборудования с поддержкой Wi-Fi 6E в мире неуклонно растет, а потребности этих устройств в широкополосном доступе к сетям связи увеличиваются с каждым днем. В России также есть производители, в частности, компания Eltex, которые анонсировали разработку точек доступа с поддержкой Wi-Fi 6E. Не исключено, что через некоторое время диапазоны частот, используемые сетями Wi-Fi сегодня, окажутся перегружены и не будут справляться с потоком данных. Возможно, что для регулятора это послужит поводом к принятию решения о передаче частот диапазона 6 ГГц для нужд Wi-Fi.

В современном мире развитие технологий, в частности Wi-Fi, – это непрерывный процесс. Сегодня полным ходом идет разработка нового стандарта Wi-Fi 7, обещающего дальнейшее увеличение скорости передачи данных и расширение возможностей. ИКС

▲ Рис. 3. Страны, принявшие и рассматривающие использование диапазона 6 ГГц для сетей Wi-Fi

Анатолий Яковлев: «Мы ориентируемся на стандарты качества мировых лидеров СКС»



Высокопроизводительные СКС для ЦОДов традиционно поставляли в Россию западные вендоры. На то, чтобы занять эту нишу, претендует белорусская компания Patchwork. Подробнее – Анатолий Яковлев, директор по продажам Patchwork.

– Анатолий, расскажите вкратце о компании Patchwork.

– Компания была образована в 2014 г. единомышленниками, имеющими большой опыт работы с решениями СКС для офисных зданий и ЦОДов. Накопив экспертизу и приняв во внимание недостатки крупных производителей – отсутствие гибкости и неповоротливость, – мы поняли, что способны предложить рынку высокотехнологичные, удобные решения, которые будут наилучшим образом отвечать потребностям заказчиков. Главный в нашей компании – это заказчик, именно он движет нас вперед.

Производственные мощности Patchwork находятся в Минске (Беларусь), а основной деятельностью является производство СКС для ЦОДов, офисов, а также для тяжелых условий эксплуатации (кабельная инфраструктура базовых станций мобильной связи, радиорелейных линий, систем видеонаблюдения).

Компания обеспечивает сопровождение изделий на протяжении всего жизненного цикла: от разработки концепции до серийного производства. В составе наших решений используются высококачественные компоненты как собственной разработки и изготовления, так и ведущих мировых производителей. В структуре компании выделен центр компетенций, в котором задействованы специалисты с многолетним опытом работы в мировых производителях кабельных систем.

– В чем преимущество расположения компании на территории Республики Беларусь?

– В первую очередь отмечу высокий производственный и инженерный потенциал, который Беларусь не потеряла после распада СССР. При выпуске любой высокотехнологичной продукции главное – это высококлассные инженеры, а мы обладаем специалистами, готовыми решать задачи любой сложности.

Важно и то, что Республика Беларусь входит в ЕАЭС. В 2022 г. было принято решение об объединении реестров промышленной продукции стран этого союза, поэтому продукция, выпущенная на территории стран ЕАЭС, приравнивается к той, что произведена в России. Это наше серьезное преимущество.

– На какие целевые группы потребителей ориентированы ваши продукты?

– Основные наши заказчики – корпоративные и коммерческие ЦОДы, а также операторы мобильной связи.

Для ЦОДов мы предлагаем оптические высокоплотные решения (вплоть до 1728 оптических волокон на 1U для MTP-24), претерминированные решения на базе групповых соединителей MTP/MPO, а также претерминированные кассеты и разветвительные сборки. Возможно использование всех основных типов оптических волокон (SM, OM3, OM4, OM5) и соединителей – включая VSFF (Very Small Form Factor), специфицированных для применения в MSA-трансиверах QSFP-DD и SFP-DD. Отдельно отмечу системы организации кабелей и решения для подключения blade-коммутаторов. Наши продукты позволяют строить инфраструктуру, поддерживающие скорости вплоть до 400 GbE, в планах – поддержка 800 GbE.

Решения для операторов мобильной связи – это кабельные сборки для инфраструктуры радиоподсистемы и для подключения к портам модулей электрического изменения угла наклона антенн (RET).

– В ЦОДах доминируют оптические системы. Какие их характеристики наиболее важны?

– Два основных параметра, над которыми нужно постоянно работать для получения качественного продукта, – это уровни затухания и возвратных потерь. Производители стремятся сделать значения данных параметров как можно меньше, поскольку от этого зависит возможность поддержки высоких скоростей. Мы построили процесс производства таким образом, что эти параметры намного ниже, чем требуется стандартами.

Оптика не только вытесняет «медь» из ЦОДов, она также меняет архитектуру и топологию организации СКС. Новые технологии, такие как параллельная передача данных, предъявляют новые требования к количеству волокон в соединителях, а постоянно растущие вычислительные мощности заставляют разрабатывать все более и более высокоплотные решения. Поэтому при разработке наших продуктов мы считаем важным обеспечить поддержку максимально возможного количества сценариев перехода на высокоскоростные протоколы, что позволит

нашим заказчикам существенно снизить риски в процессе миграции.

– Насколько ваши продукты по своим характеристикам сопоставимы с решениями мировых лидеров рынка высокопроизводительных СКС для ЦОДов – CommScope, Panduit, Huber+Suhner, Corning?

– На уровне компонентов (оптические сборки, модули, cassette, коммутационные шнуры) наши решения ничем не уступают продукции известных мировых производителей. По уровню затухания и возвратных потерь наши продукты сопоставимы, а в ряде случаев даже превосходят лучшие мировые аналоги.

На стандарты качества названных вами компаний мы и ориентировались при создании производства. Поэтому с самого начала использовали только самое современное и высокотехнологичное оборудование. Сотрудники компании имеют высочайшую квалификацию и, поверьте, отличаются в лучшую сторону от персонала вышеупомянутых компаний в Индии, Мексике и Китае. Сквозная система контроля качества на всех этапах производства не имеет аналогов в РФ и удовлетворяет всем мировым требованиям высокотехнологичного производства. А современные методы управления позволяют своевременно выявлять актуальные рационализаторские предложения по усовершенствованию процессов производства.

В начале 2020 г. Patchwork встала на путь Lean, или путь бережливого производства. Для нас Lean – это минимизация всех видов потерь, рациональное использование ресурсов, постоянные улучшения и усовершенствования, а также философия или часть культуры, менталитет, способ мышления всех сотрудников компании (Lean-DNK). За два с половиной года внедрения Lean существенно повысился уровень удовлетворенности наших заказчиков и собственных сотрудников компании. Но понимаем, что мы еще в самом начале пути, любой процесс всегда можно улучшить. Поэтому мы называем Lean путем и намерены постоянно добиваться все большей вовлеченности сотрудников в применение существующих и новых инструментов Lean.

– Если говорить о медножильных решениях, то для каких задач они используются в современных ЦОДах? Что предлагает Patchwork?

– Спектр задач, для которых используются медные компоненты СКС, в ЦОДах достаточно широк. Это подключение различных устройств: от нетребовательных к скорости передачи данных устройств KVM и PDU до камер видеонаблюдения высокой четкости с питанием по PoE. Появление новых мультигигабитных протоколов также способно продлить срок службы медной СКС в ЦОДе. В портфеле компании представлены модульные решения стандартной и повышенной плотности категорий 6 и 6А в экранированном и неэкранированном исполнении.

– В случае применения высокоплотных СКС крайне важно удобство их эксплуатации. Как это требование выполняет Patchwork?

– В нашем портфеле решений есть так называемый базовый продукт: универсальная коммутационная панель FLEX TRAY, которая позволяет не только построить универсальную среду передачи данных (оптика и «медь»), но и

применить различные решения для организации кабельных линий.

Что касается высокоплотных решений, мы рекомендуем заказчикам использовать соединители с хвостовиком типа Push-Pull-Boot, который одновременно является и ограничителем изгиба кабеля, и экстрактором. Общая особенность всех оптических соединителей платформы Push-Pull – возможность смены полярности в полевых условиях без риска повреждения оптических волокон.

Это решение получило очень хороший отклик у наших заказчиков, и они активно его применяют. Использование продуктов Push-Pull упрощает эксплуатацию и, самое главное, сводит к минимуму риски несанкционированного отключения кабельных линий от тракта сети, что повышает уровень надежности объектов.

– Над чем сейчас работают в R&D-отделах Patchwork?

– Наша основная задача – предлагать заказчикам удобные, качественные решения для построения кабельной инфраструктуры. Удобство эксплуатации такой инфраструктуры – одно из важнейших свойств предлагаемых решений. В данный момент работаем над решениями высокой плотности для организации СКС в ЦОДах, над решениями для подключения рабочих мест по оптическому волокну при построении офисных СКС, а также над системой управления кабельной инфраструктурой. Это очень важный элемент для эффективной эксплуатации СКС.

– Могли бы вы привести примеры проектов, реализованных в ЦОДах?

– Различные виды кабельных систем Patchwork уже успешно эксплуатируются многими российскими компаниями телекоммуникационной, финансовой, газовой и машиностроительных отраслей. Если говорить о решениях для ЦОДов, то все вышеупомянутые решения активно применяются у наших заказчиков. Один из интересных проектов, который сейчас находится в стадии реализации, связан с построением кабельной инфраструктуры на 400 GbE с применением высокоплотного решения (256 волокон на 1U) с соединителями очень малого форм-фактора (VSFF) и MTP-16.

– Как Patchwork видит свою задачу с учетом прекращения работы в России западных производителей СКС?

– К сожалению, ситуация, которая сложилась на нашем рынке, – уход признанных экспертов в области создания кабельной инфраструктуры, компаний с большой историей и высококачественными продуктами, – поставила многих заказчиков в затруднительное положение. Они потеряли возможность построения сложной, нестандартной кабельной инфраструктуры. Наша задача – предоставить заказчикам высококачественные продукты, которые позволят решить любую возникшую у них задачу. За счет накопленной за многие годы экспертизы и с помощью разработанных нами решений мы способны справляться с самыми сложными задачами.

Удаленный доступ через VPN в новой реальности

Николай Носов

В условиях санкционных ограничений и регуляторного давления для удаленной работы предпочтительнее использовать российские решения. Драйвером роста рынка VPN станет резко увеличившийся спрос на услуги ЦОДов и облачные сервисы.

Новый стандарт работы – «удаленка»

Пандемия и карантинные меры привели к резкому и массовому переходу на удаленный режим работы. Преимущества использования компьютерных технологий оценили все. Бизнес экономит на аренде помещений, организации рабочих мест в офисе и командировочных расходах, сотрудники не тратят время и деньги на дорогу до работы и обратно. Поэтому и после отмены карантинных ограничений люди не стали спешить возвращаться в офисы. В лексикон прочно вошло слово «видео-конференц-связь» (ВКС), написание которого до сих пор вызывает споры. Удаленная работа стала нормой нашей жизни и одним из основных критериев при трудоустройстве. Так, по данным исследования «Группы ГАЗ», при выборе работодателя значимость возможности удаленной работы отмечают 75% женщин и 60% мужчин (рис. 1).

А 60% респондентов заявили, что не готовы работать только в офисе (рис. 2).

Причем особенно важна возможность удаленной работы для молодежи – об этом заявили более 70% респондентов в возрасте от 21 до 40 лет, прежде всего айтишники (77%), пиарщики, юристы и HR-специалисты (рис. 3).

Существующие риски

С началом пандемии бизнес-процессы перестраивали в авральном порядке, зачастую не задумываясь об информационной безопасности. Неудивительно, что массовый переход на уда-

ленную работу самых разных предприятий и организаций вызвал всплеск киберпреступности.

Ситуация значительно осложнилась после февраля 2022 г. из-за геополитической обстановки. С одной стороны, приостановили или прекратили свою деятельность в нашей стране международные компании, во многом обеспечивавшие безопасную удаленную работу. Ушла занимавшая лидирующее положение на российском рынке сетевого оборудования компания Cisco. Опасаясь вторичных санкций, практически заморозила активность в России китайская Huawei, которую рассматривали как главного кандидата на замену американского гиганта. Приостановила продажи и поддержку клиентов лидер на рынке безопасных виртуальных рабочих мест компания Citrix. Отказывает в продаже лицензий Microsoft.

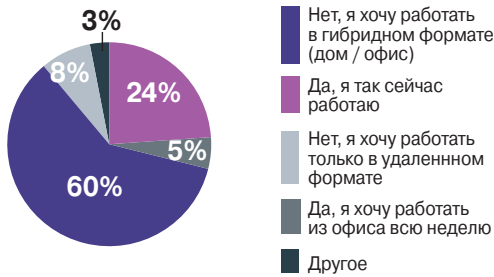
С другой стороны, стране объявили настоящую войну в киберпространстве. Россия стала самой атакуемой страной в мире. В зоне риска оказались все российские компании независимо от размеров и вида деятельности. Для того чтобы попасть под атаку, достаточно иметь домен в зоне .ru. При этом атаки проводят не только антироссийски настроенные хакеры-любители, но и, как говорится в заявлении МИД России, украинские спецподразделения информационно-технического воздействия и «армия кибернаемников, перед которыми стоят конкретные боевые задачи, нередко граничащие с открытым терроризмом».

Рис. 1. Удаленная работа как аргумент в пользу выбора работодателя ▶



Источник: gazgroup.ru

Готовы ли Вы работать из офиса на постоянной основе?



Источник: gazgroup.ru



Источник: gazgroup.ru

◀ Рис. 2. Готовность работать из офиса на постоянной основе

◀ Рис. 3. Топ-5 сфер деятельности, где респондентам важна возможность работать удаленно

Защита канала связи

Системы удаленного доступа – привлекательная цель для преступников. Под угрозой как передаваемая по внешней сети информация, так и конечные устройства – компьютеры пользователей.

При удаленной работе прежде всего надо организовать канал связи. До каждого регионального офиса и тем более сотрудника выделенную линию не проведешь – слишком дорого. Остается использовать сети общего доступа и развертывать поверх них виртуальные частные сети (Virtual Private Network, VPN). Самый простой и дешевый способ – через интернет.

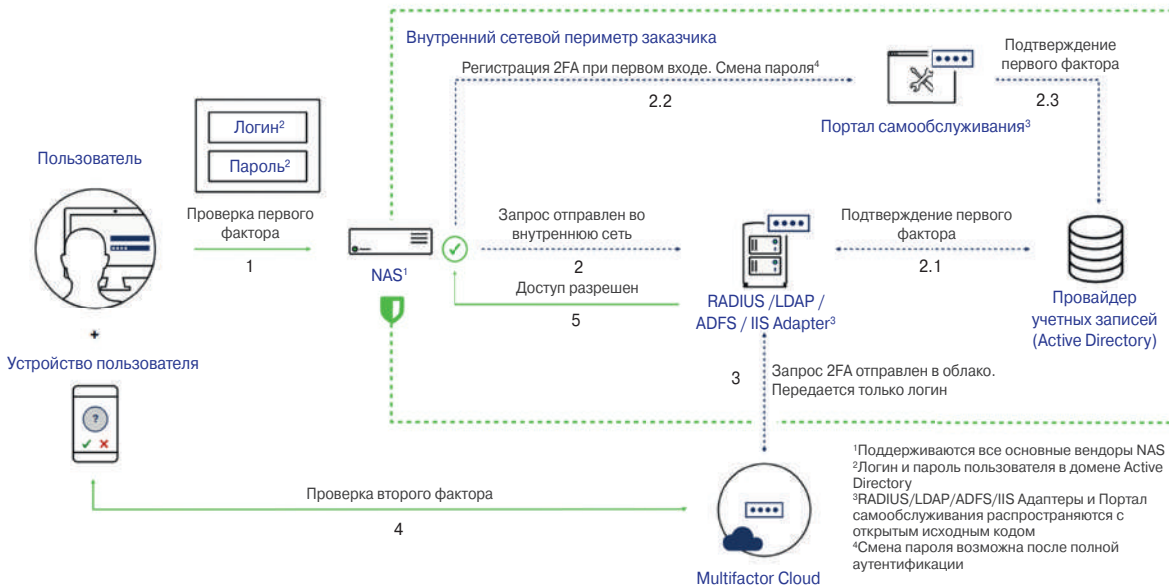
Общедоступная сеть накладывает ограничения – мало организовать канал, нужно еще и шифровать трафик. Чем сложнее алгоритмы шифрования и выше надежность защиты, тем медленнее идет передача, ведь данные надо сначала зашифровать, а потом расшифровать, и на это тратятся ресурсы находящихся по обе стороны туннеля компьютеров. Недостаток компенсируется использованием специализированных программно-аппаратных средств для шифрования – криптографических шлюзов (VPN-шлюзов). В числе российских решений можно назвать

криптошлюзы «С-Терра Шлюз» (производства компании «С-Терра СиЭсПи»), АПКШ «Континент» («Код Безопасности»), «Атликс-VPN» («НТЦ Атлас») и программно-аппаратные комплексы, в которые помимо криптошлюза входит межсетевой экран: ViPNet Coordinator HW («ИнфоТекС») и ФПСУ-IP («Амикон» при участии «ИнфоКрипт»).

Для организации безопасного зашифрованного канала применяются и программно-аппаратные комплексы с более широким функционалом, включающим в себя VPN-шлюз, межсетевой экран, средства обнаружения и предотвращения вторжений. В ряду таких систем можно отметить Dionis-NX («Фактор-ТС»); Diamond VPN/FW (ТСС); Altell Neo («АльтЭль»); «Застава» («Элвис-Плюс»). Последний из перечисленных комплексов может служить также центром управления политиками безопасности.

Режим полного туннелирования на основе аппаратных криптошлюзов, установленных на обеих сторонах канала, обеспечивает наибольшую безопасность и производительность, но из-за высокой стоимости применяется в основном для защиты каналов связи с филиалами и другими удаленными площадками компаний.

Высокоуровневая схема разрешения



◀ Рис. 4. Общая схема системы Multifactor

Источник: «Мультифактор»

Для работы сотрудников проще использовать программную реализацию механизмов межсетевой фильтрации и шифрования. В условиях жестких санкций на поставку микропроцессоров и других ИТ-компонентов для рынка связи программные решения приобретают особую актуальность. «Наша компания, как и многие другие участники рынка средств информационной безопасности, столкнулась с ограничениями на поставку комплектующих для программно-аппаратных комплексов. Но для нас это не стало проблемой, поскольку мы предлагаем продукты также в виртуализированном исполнении: виртуализированный шлюз безопасности и виртуализированный межсетевой экран нового поколения», – отметил заместитель генерального директора компании «ИнфоТеКС» Дмитрий Гусев.

Помимо обеспечения безопасного доступа сотрудников к корпоративной сети (Remote-access VPN), защищенные каналы используются для объединения в общую сеть нескольких филиалов одной организации (Intranet VPN), для сетей, к которым подключаются заказчики или клиенты (Extranet VPN). Настройку и поддержку работы защищенных каналов осуществляют интеграторы или телеком-операторы, предоставляющие оборудование в аренду.

Многофакторная аутентификация

Поскольку устройство, с которого сотрудник подключается к информационной системе предприятия, находится вне периметра безопасности организации, существует риск несанкционированного доступа к VPN-каналу. Простой аутентификации – проверки подлинности пользователя путем сравнения введенных им логина и пароля с сохраненными в базе данных организации – становится недостаточно. Не помогут даже повышенные требования к используемым символам и длине пароля – его могут перехватить незаметно, внедрив зловред на устройство пользователя. Риск компрометации пароля усиливают фишинговые атаки и применение преступниками средств социальной инженерии. Да и службы безопасности нередко допускают халатность – не удаляют из базы логины и пароли уволившихся сотрудников. Поэтому правиль-

ный подход – использование многофакторной аутентификации. В качестве второго фактора проверки подлинности сотрудника и правомерности его доступа задействуют токены, биометрию, push- и sms-сообщения, подтверждение через социальные сети или телефон.

Компании, производящие средства двухфакторной аутентификации, предоставляют свои услуги в виде готовой платформы, устанавливаемой в защищаемом периметре заказчика, а также в виде облачного сервиса (SaaS). Пример такой реализации – продукт Multifactor компании «Мультифактор» (рис. 4).

После проверки логина и пароля запрос отправляется во внутреннюю сеть – на сервер аутентификации, который служит единым центром администрирования всех процессов проверки подлинности для всех приложений и сервисов. Промышленные серверы такого типа поддерживают целый набор методов аутентификации. Как правило, это OATH HOTP, TOTP, OCRA, PKI-сертификаты, RADIUS, LDAP, обычный пароль, SMS, CAP/DPA. Каждый ресурс, использующий сервер аутентификации, может задействовать метод, который требуется именно ему. Логин пользователя передается в облако, через которое осуществляется проверка второго фактора.

Среди других российских решений двухфакторной аутентификации можно выделить продукты JaCarta компании «Аладдин Р.Д.» и сервис AUTHN.AS от компании RCNTEC, входящие в Единый реестр российских программ для ЭВМ и баз данных.

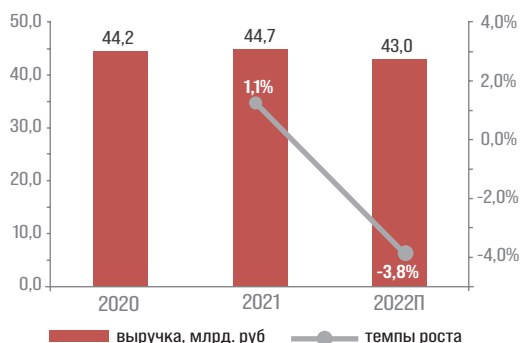
Прогноз развития рынка

В годы пандемии, по данным iKS-Consulting, российский рынок услуг VPN рос на 1–2% в год (рис. 5). Геополитические изменения и санкции привели к необходимости оптимизации затрат, что сказалось и на бюджетах ИТ-служб. Прогнозируется, что по итогам 2022 г. рынок сократится на 3,8%.

Услуги VPN предлагают в основном российские операторы связи, а среди зарубежных заметную долю (9%) в 2021 г. имела только французская Orange Business Services, которая может сильно пострадать из-за ухода с российского рынка своих клиентов – зарубежных компаний. Игроков много, конкуренция высокая. Лидирующие позиции (45%) занимает «Ростелеком», а региональные операторы представлены слабо, и их доля, по мнению аналитиков iKS-Consulting, в ближайшие годы будет сокращаться из-за обострения конкуренции как с федеральными операторами, так и с интеграторами.

Сложная экономическая ситуация отражается на прогнозах развития сегмента VPN. Рынок насыщен, проникновение услуг VPN на внутрирегиональном рынке в ряде отраслей превышает 50%, но все же потенциал для роста есть, напри-

Рис. 5. Динамика объема рынка услуг VPN (все технологии) в РФ, 2020–2022 гг., млрд руб. ►



Источник: iKS-Consulting

Отрасль (согласно ОКВЭД)	Тип подключений VPN, %	
	Межрегиональные	Внутрирегиональные (внутригородские)
Сельское, лесное хозяйство, охота, рыболовство и рыбоводство	10,1	14,8
Добыча полезных ископаемых	21,2	37,2
Обрабатывающие производства	21,8	36,4
Строительство	11,2	20,6
Торговля оптовая и розничная, ремонт автотранспортных средств и мотоциклов	27,8	51,3
Транспортировка и хранение	18,5	43,0
Деятельность гостиниц и предприятий общественного питания	18,4	24,4
Деятельность в области информации и связи	26,6	41,2
Деятельность финансовая и страховая	48,7	64,7
Деятельность по операциям с недвижимым имуществом	11,2	16,3
Деятельность профессиональная, научная и техническая	15,7	23,6
Деятельность административная и сопутствующие дополнительные услуги	14,1	22,3
Государственное управление и обеспечение военной безопасности; социальное обеспечение	13,4	19,1
Деятельность в области здравоохранения и социальных услуг	23,2	25,8
Деятельность в области культуры, спорта, организации досуга и развлечений	8,6	9,0
Ремонт компьютеров, предметов личного потребления и хозяйственно-бытового назначения	5,8	58,1
Сектор информационно-коммуникационных технологий	30,6	52,5
Сектор контента и средств массовой информации	13,7	19,1
Отрасль информационных технологий	30,9	46,5

◀ Уровень проникновения VPN разных типов в разрезе основных отраслей, 2020 г.

Источник: опрос Минцифры России, более 190 тыс. средних и крупных предприятий РФ, 2020 г.

мер, за счет все еще слабо используемых межрегиональных VPN-подключений. Особенно заметен контраст между использованием внутрирегиональных и межрегиональных VPN-подключений в торговле (см. таблицу).

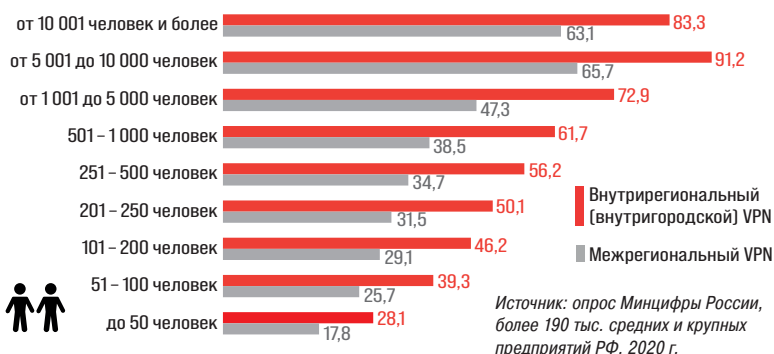
Рост возможен и за счет более широкого проникновения услуг VPN в сегмент среднего и малого бизнеса (рис. 6). Да и крупный бизнес, активно применяющий VPN, столкнется с проблемами модернизации, в том числе из-за прекращения поддержки оборудования ушедшими с российского рынка компаниями.

Дефицит оборудования тормозит развитие корпоративных on-premise решений и повышает привлекательность облачных сервисов. Резко возросший спрос на услуги ЦОДов и облачные сервисы и, как следствие, на защиту каналов связи станет драйвером роста рынка VPN.

Ставка на российское

Прошли те времена, когда наиболее беспечные банки выходили из внутренней сети в интернет без NAT и межсетевых экранов – с «белых» IP-адресов. Теперь это такая же дикость, как квартира без замка в многоэтажке. Сегодня «замки» и защищенные каналы используют все.

Уход с российского рынка западных поставщиков средств защиты каналов связи усложнил использование их аппаратных и программных продуктов. Конечно, можно ничего не предпринимать и ждать окончания срока действия лицензий, надеясь, что к тому времени ситуация нормализуется и западные вендоры вернуться в Россию. Можно переходить на продукты компаний, не покинувших российский рынок, но нет



Источник: опрос Минцифры России, более 190 тыс. средних и крупных предприятий РФ, 2020 г.

гарантий, что изменения в геополитической обстановке не подтолкнут к уходу и их.

До начала спецоперации на Украине перспективным вариантом замены выглядело использование свободного ПО, но в последнее время в этих программах выявлены десятки специальных, ориентированных на конкретные страны закладок, что заставляет относиться к СПО с осторожностью. Многие компании после февраля даже прекратили обновлять такие продукты.

Интерес к российским решениям стимулирует Указ Президента РФ № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации», согласно которому с 1 января 2025 г. иностранное ПО запрещается использовать компаниям с госучастием, ЗОКИИ и органам государственной власти. Вариантов развертывания новых и поддержки старых VPN много. Каждая компания выбирает, исходя из оценки рисков и уже сделанных инвестиций. Наиболее безопасный путь – использовать российские продукты. ИКС

▲ Рис. 6. Уровень проникновения VPN разных типов в разрезе предприятий различного размера, 2020 г., %

EMILINK: собственное производство = оптимальная цена + контроль качества

К своему 15-летию ГК EMILINK подошла с сильной производственной базой и портфелем комплексных решений для инженерной инфраструктуры ЦОДов. О развитии компании и рынка в целом мы побеседовали с основателем EMILINK Андреем Зуевым.



– Что сегодня представляет собой ГК EMILINK?

– Мы прошли большой путь и стали крупной мультипроизводственной компанией. За 15 лет была создана мощная производственная база. Последние годы, учитывая тенденции рынка к импортозамещению, мы развиваемся ускоренными темпами. Семь производственных площадок выпускают широкий ассортимент продукции для отрасли ЦОДов и телеком-рынка – как непосредственно для операторов, так и для системных интеграторов. По некоторым направлениям EMILINK занимает ведущие позиции. Так, компания является крупнейшим производителем волоконно-оптических патчкордов на всем постсоветском пространстве. По сочетанию сроки/цена/качество мы – лидеры в РФ в сегменте шкафов и систем изоляции для ЦОДов. ГК EMILINK принадлежит несколько торговых марок (NTSS, КОСТРОМАКАБЕЛЬ), которые имеют свою дистрибьюторскую сеть в России и странах СНГ.

– В июле 2022 г. вы открыли новую площадку по металлообработке. Насколько она позволила увеличить объем выпускаемой продукции?

– Металлообработкой мы занимаемся десять лет и за это время добились неплохих результатов. Открытие новой площадки не спонтанное решение, обусловленное недавними событиями. Мы планировали рост производства заранее. Переезд в новое здание – это и расширение станочного парка, и увеличение штата сотрудников. Сегодня станки загружены на 50%, а значит, мы готовы минимум вдвое увеличить объем производства. Кроме того, площади предоставляют возможность для дальнейшего роста: по моим прогнозам, в ближайшие два года мы должны увеличить собственные производственные мощности более чем в три раза – это обработка примерно 600 т листового металла в месяц.

Мы также развиваем НИОКР. За последнее время наша команда пополнилась конструкторами и продукт-менеджерами высочайшего класса из западных компаний, ушедших с российского рынка. Эти специалисты более десятка лет трудились на зарубежных вендоров, а сейчас всю свою экспертизу вкладывают в наши текущие и будущие разработки. Наши продукты выходят на один уровень с решениями международных брендов, а в некоторых технических моментах мы их превосходим.

– Компания планировала дополнить свои решения системами ИБП и кондиционирования. Как идет этот процесс?

– Многие наши партнеры желают получать моновендорное решение для инженерной инфраструктуры ЦОДов, которое должно включать в себя системы пожаротушения, ИБП и кондиционирования, а также блоки PDU. Такие блоки мы производим в Костроме. Сегодня, учитывая наши лидерские позиции в производстве и поставках шкафов для ЦОДов, все известные в России производители и поставщики добавочного оборудования готовы сотрудничать с нами для реализации проектов любой сложности, подключая свою инженерную компетенцию, – как по схеме OEM, так и под своим брендом. Поэтому мы можем предложить заказчику любые продукты по рыночным ценам в рамках комплексной поставки, обеспечивая работу в формате одного окна с системной гарантией на все решение в комплексе.

– Сегодня возникли серьезные проблемы на рынке СКС для ЦОДов, с которого ушли все основные зарубежные поставщики. Насколько ваши решения по своему функционалу и качеству могут использоваться для построения высокопроизводительной сетевой инфраструктуры ЦОДов?

– Мы много лет развиваемся как производитель и поставщик СКС-решений под брендом NTSS. При этом мы имеем глубокую специализацию в оптических решениях для внутренней сетевой инфраструктуры: сами производим оптический кабель, из него делаем кабельные сборки и оптические шнуры для высокоплотных решений (которые доминируют в ЦОДах), сами же отливаем пластиковые аксессуары и предлагаем большой ассортимент решений для организации кабельного хозяйства. Кроме того, мы сами производим медные патчкорды, что дает нам независимость и оперативность в любых сложных проектах, где требуются высокая скорость поставки и жесткий контроль качества. Всю свою экспертизу и продукты предлагаем на рынке ЦОДов. И считаем, что наши решения не уступают по качеству продуктам мировых брендов, но при этом более выгодны по цене.

– За последние полгода вы наверняка много общались с представителями крупнейших ЦОДов. Насколько



их устраивают качество, функционал и стоимость ваших изделий? Над чем еще предстоит поработать?

– Мы никогда не останавливаемся в развитии и улучшении своих продуктов, всегда прислушиваемся к отзывам заказчиков и партнеров. Конечно, универсальных решений не бывает, многое зависит от навыков службы эксплуатации, их привычек к работе с разными конструкциями шкафов и другого оборудования различных вендоров. Мы внимательно изучаем каждый отзыв, и если замечания действительно веские, то дорабатываем конструкции. За семь лет производства шкафов ПРОЦОД в данной серии сменились шесть поколений. Каждое подвергалось серьезной доработке на основе обратной связи от заказчиков, после долгой эксплуатации непосредственно в ЦОДах. Мы считаем, что наш конструктив практически идеален, но поскольку нет ничего абсолютно идеального, продолжаем совершенствоваться.

Как я уже говорил, в нашу команду влились высококлассные специалисты, которые знают, как должен работать продукт/компания для достижения максимально слаженного взаимодействия с партнерами и заказчиками. Кроме того, у нас большой пул менеджеров по продажам и сопровождению, и каждому заказчику выделяется персональный менеджер. Этот менеджер отрабатывает все вопросы, которые связаны с текущими или будущими проектами, привлекая весь наш производственный и инженерный потенциал.

– Насколько рост спроса на российские продукты может увеличить темпы вашего роста?

– На протяжении 15 лет мы развивались, опираясь на собственные силы. Наш рост в среднем составлял 30–40% в год. Считаю, если эти показатели превышаются в разы, компания может начать «болеть»: не будет успевать качественно отрабатывать проекты, нанимать и готовить специалистов, следить за бизнес- и производственными процессами, наличием продукции на складах, увеличивать производственные мощности. Наконец, могут возникнуть трудности с выполнением финансовых обязательств – если речь идет о кредитовании проектов и т.д.

Да, на нашем рынке есть игроки, которые растут быстрее, но не за счет собственного потенциала, а за счет других производственных компаний, предлагая продукт не

«со своего станка», а по OEM-схеме. Но в такой схеме растет добавочная стоимость финального продукта, и за это расплачивается конечный потребитель. Почему наши цены одни из самых выгодных? Потому что мы производим сами, адекватно оцениваем свой труд и являемся первоисточником в поставке. Этот год не исключение – мы берем заказов столько, сколько готовы выполнить без надрыва и предоставить максимальное надежное и качественное решение партнерам и заказчикам. Мы на рынке не с целью урвать и воспользоваться ситуацией. Нам важна репутация.

– Каковы ваши планы освоения зарубежных рынков, прежде всего стран СНГ?

– В этом году у нас появился эксклюзивный дистрибьютор в Республике Беларусь, кроме этого мы намерены открыть собственные офисы и склады в Казахстане и Узбекистане.

– Каким вы видите дальнейшее развитие российского рынка ЦОДов в целом и рынка решений для их инженерной инфраструктуры в частности?

– Безусловно, сейчас идет серьезная перестройка отечественного рынка решений для ЦОДов. Для многих поставщиков и производителей это колоссальный шанс, который может не выпасть больше никогда. В целом же рынок испытывает большие перегрузки в связи с переходом на новые рельсы, пересмотром проектов, изменением номенклатуры продуктов и самих решений. Но отрасль цодостроения, как и любой живой организм, пробьет себе выход к солнцу.

Потребность в ЦОДах сегодня постоянно увеличивается, появляются все новые проекты, и отрасль ЦОДов – один из понятных для нас источников финансирования. Считаю, что до конца текущего года рынок в основном перестроится в соответствии с новой реальностью. В следующем году возможны точечные проблемы с качеством или срочной заменой каких-либо деталей, компонентов или решений в целом, но до конца 2023 г. рынок предложения полностью стабилизируется.

ЦОДы и облака: трудности и надежды

Николай Носов

Стремительный рост спроса на облачные услуги становится основным драйвером развития коммерческих ЦОДов. Санкции – это серьезный вызов, но в целом рынок облаков справится с возникшими сложностями.

В этом году на форуме «ЦОД», организованном в Москве «ИКС-Медиа», беспрецедентно много внимания было уделено облакам. И это неудивительно: доля облаков в объеме российского рынка ЦОДов за последние годы сильно выросла – с 34% в 2018 г. до 43% в 2021 г. (данные iKS-Consulting), чему в немалой степени способствовали карантинные ограничения во время пандемии. Однако и с их отменой отката не произошло – по прогнозам iKS-Consulting, в 2022 г. эта доля составит 44%. Недалек тот день, когда облачные сервисы обгонят colocation и станут основными услугами коммерческих ЦОДов.

Облака в новой реальности

С уходом из России зарубежных вендоров, невозможностью приобрести их аппаратные и программные продукты и резким ростом количества и интенсивности кибератак облака, по словам руководителя направления облачных продуктов «Мегафона» Александра Осипова, оказались в новой реальности. А. Осипов выделил новые факторы, влияющие на развитие облачного рынка: трудности с поставками «железа», необходимость импортозамещения оборудования и ПО, обеспечение кибербезопасности.

Проблемы «новой реальности» особенно сильно бьют по крупным корпоративным ЦОДам, усложняя техническое обслуживание продукции ушедших с рынка зарубежных вендоров. В частности, продукция Cisco и Huawei, как отметил директор центра сетевых решений компании «Инфосистемы Джет» Сергей Андронов, доступна теперь только по крайне ненадежной схеме параллельного импорта. Поэтому во многих корпоративных ЦОДах возникли серьезные трудности с реализацией современных технологий EVPN (Ethernet Virtual Privacy Network),



Источник: «Инфосистемы Джет»

виртуально расширяемых локальных сетей и мультисегментирования в сетях передачи данных (рис. 1).

Да и высокоскоростные транспортные маршрутизаторы российскими производителями пока не освоены. В результате крупные корпоративные дата-центры, ориентированные на мультисервисную среду, на быстрое перестроение предоставляемых сервисов, обмен между виртуальными машинами, находящимися в разных геолокациях, из-за отсутствия сетевого оборудования перестали развиваться.

Облака рассредоточиваются...

Проблему С. Андронов предлагает решать на уровне изменения архитектуры – перехода от централизованной обработки данных к децентрализованной. В сегодняшней ситуации, когда высокопроизводительное ИТ-оборудование стало труднодоступным, выходом может быть использование концепции Edge Computing, согласно которой небольшие дата-центры выносятся на границу сети, к месту сбора данных. В них и происходит основная обработка, а в головной ЦОД, разгружая каналы, передаются лишь информационные «выжимки». «Это тот

▲ Рис. 1. Текущая ситуация на рынке



В сегодняшней ситуации, когда высокопроизводительное ИТ-оборудование стало труднодоступным, выходом может быть использование концепции Edge Computing, согласно которой небольшие дата-центры выносятся на границу сети, к месту сбора данных. В них и происходит основная обработка, а в головной ЦОД, разгружая каналы, передаются лишь информационные «выжимки».



▲ Рис. 2. ЦОДы инфраструктуры МТС

тренд, который видим на рынке сейчас. Мы получили множество запросов на строительство малых ЦОДов, от Дальнего Востока до Калининграда», – пояснил С. Андронов. В качестве таких edge-ЦОДов «Инфосистемы Джет» считает целесообразным использовать контейнерные решения, которые ускоряют и упрощают создание объекта и ввод его в эксплуатацию. Например, весной текущего года для будущего свинокомплекса «Русагро» компания развернула контейнерный ЦОД за 120 дней.

Российские операторы связи, хотя и имеют запасы оборудования, также следуют тренду на децентрализацию, стараясь приблизить свои облачные сервисы обработки к местам сбора/генерации информации у клиентов.

Так, МТС в дополнение к своей базовой федеральной инфраструктуре поддержки мобильной связи покрывает страну дата-центрами, обеспечивающими доступность посто-

янно расширяющегося спектра облачных услуг (рис. 2).

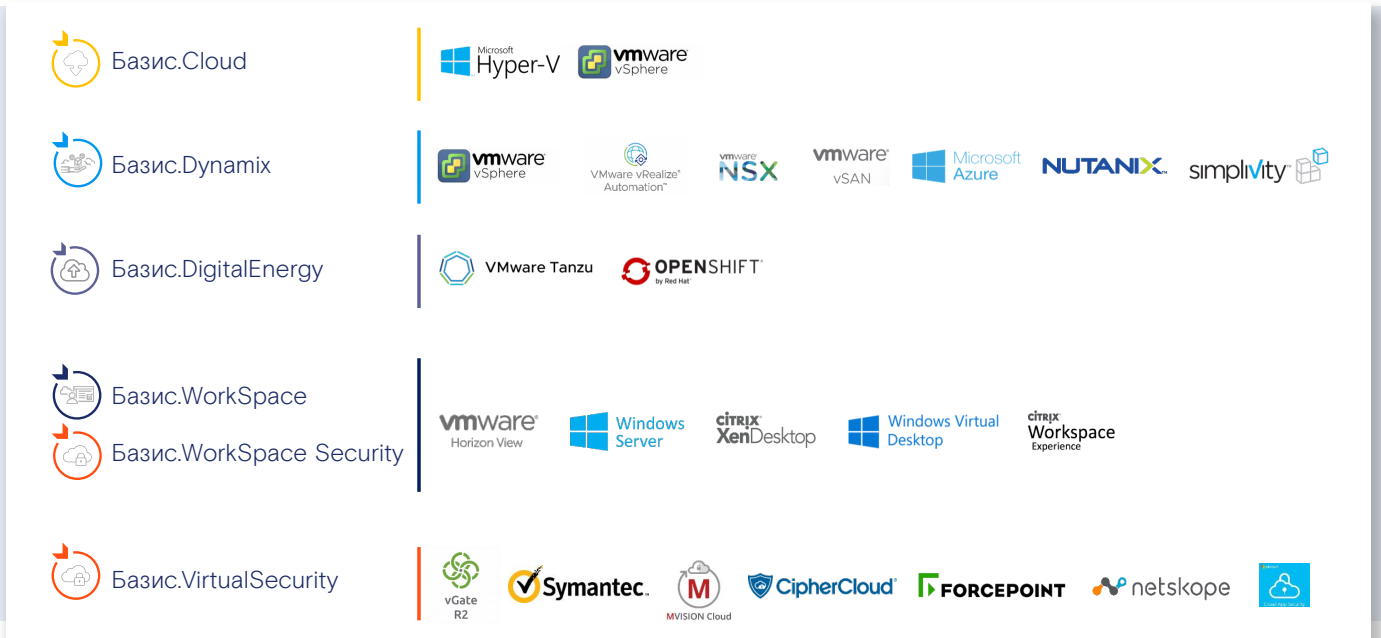
Сеть из подмосковных мегаЦОДов «Авантаж» в Лыткарине и GreenBushDC в Зеленограде, как сообщил директор по облачным продуктам #CloudMTS Михаил Соловьев, дополняется модульными ЦОДами в крупных региональных центрах (в промышленной эксплуатации уже находятся МЦОДы в Санкт-Петербурге, Нижнем Новгороде и Новосибирске), edge-ЦОДами в больших городах и совсем небольшими «дальними» Far edge-объектами в локациях с большим трафиком или в клиентских 5G- или LTE-проектах. На базе своей распределенной сети дата-центров МТС предоставляет бизнесу облачное решение, включающее развитую экосистему облачных сервисов и возможность создания частных облаков клиентов, причем на собственной системе виртуализации и облачной платформе.

... а платформы сосредоточиваются

Помимо тенденции к децентрализации на облачном рынке можно увидеть и тенденцию к интеграции. Так, компания «Базис», объединившая трех известных игроков российского рынка – «Скала софтвар», «Диджитал энерджи» и одного из старейших российских разработчиков решений на базе OpenStack компанию «Тионикс», интегрировала и их продукты: программно-аппаратные комплексы «Скала-Р» от «Скала софтвар», конвейер по производству приложений для разработчиков от «Диджитал энерджи» и имеющую необходимые сертификаты российских регуляторов облачную платформу «Тионикс». «Объединение компаний позволило «Базису» стать безопасным и надежным игроком рынка», – отметил директор по

Не все российские компании могут самостоятельно и безболезненно перейти на импортозамещающие решения. Задачу упрощает переход в облако, где процесс миграции поможет наладить облачный провайдер, который в этом случае становится центром компетенций.





Источник: «Базис»

работе с партнерами компании «Базис» Дмитрий Дворцов. Предлагаемые рынку продукты охватывают практически весь спектр решений в области виртуализации и дают возможность заместить продукты ушедших из России мировых вендоров (рис. 3).

Так, используя «Базис.Cloud» – облачную платформу для виртуализации серверов и систем хранения данных, – можно обойтись без Microsoft Hyper-V и VMware vSphere; динамическая инфраструктура для управления виртуальными машинами и контейнерами «Базис.Dynamix» освободит от необходимости применять соответствующие решения Nutanix, Microsoft Azure и VMware; средство защиты информации систем виртуализации и облачных платформ «Базис.Virtual Security» может послужить заменой продуктов Symantec, CipherCloud, Forcepoint. Причем решения для обеспечения информационной безопасности сертифицированы ФСТЭК, что расширяет сферу их применения на российском рынке и является конкурентным преимуществом перед продуктами оставшихся в России зарубежных вендоров.

Впрочем, и у зарубежных продуктов по информационной безопасности ЦОДов есть свои козыри. Так, плюс решений Check Point – высокая скорость обработки информации, которая достигается благодаря использованию специализированных аппаратных ускорителей, разгружающих центральный процессор от решения задач ИБ, и динамической балансировки нагрузки между шлюзами безопасности.

Параллельный облачный импорт

Не все российские компании могут самостоятельно и безболезненно перейти на импортоза-

мещающие решения. Задачу упрощает переход в облако, где процесс миграции поможет наладить облачный провайдер, который в этом случае становится центром компетенций. Ведь провайдер имеет запас ресурсов, экспертизу по разработке решений, план действий на случай непредвиденных ситуаций и готовый набор продуктов. Именно такую позицию занимает ЦОД Охуген. По словам его директора департамента развития баз данных Ивана Тимофеева, Охуген поможет провести аудит лицензий, составит план и проведет тестовую миграцию, перенесет бизнес-процессы в облако и даже оптимизирует их на этапе переноса.

Для компаний, не имеющих возможности перейти на импортозамещающие продукты, Охуген предлагает базы данных Oracle и решения SAP из своего облака. Получается своего рода параллельный импорт облачных услуг, где вся ответственность за поддержку решений ложится на российского облачного провайдера.

Китайские облака в качестве замены ушедших с нашего рынка западных не завоевали широкой популярности и по-прежнему используются в основном китайскими компаниями, работающими на российском рынке. Поэтому основную нагрузку при удовлетворении растущего спроса на облачные сервисы должны будут взять на себя российские ЦОДы и российские облачные провайдеры. Набор их облачных сервисов постоянно расширяется и уже приближается по качеству к предложениям мировых лидеров. Значит, можно рассчитывать, что российские облачные провайдеры сумеют полностью заместить ушедших с рынка глобальных игроков. ИКС

▲ Рис. 3. Иностранное решение, замещающее продуктами «Базис»

Основные принципы масштабируемости и устойчивости облаков

Оуэн Роджерс, директор по исследованиям облачных вычислений, Uptime Institute Intelligence

С развитием облачных сервисов появилось много способов повышения их устойчивости и производительности. Потребителям важно понимать суть этих способов, поскольку частота сбоев в облаках, скорее всего, будет нарастать, как и влияние последствий таких сбоев.

Создать виртуальную машину и развернуть ИТ-приложение в публичном облаке сегодня можно за считанные минуты. Простота и гибкость существенно повышают привлекательность общедоступных облаков. Однако с ростом числа пользователей этих сервисов все больше внимания приходится уделять построению устойчивых, производительных и совместимых приложений.

Облако может быть очень удобным в несложных сценариях использования, к примеру, для развертывания веб-сайтов с некритическими задачами. Однако если необходимы, скажем, высокая устойчивость и низкая стоимость, то нередко оказывается, что выполнить эти требования в публичных облаках весьма трудно.

В настоящее время не существует стандартной архитектуры для облачных приложений: нет «наилучшего» подхода, нет «идеальной» комбинации инструментов, местоположения, поставщиков или сервисов. Пользователи внедряют различные платформы, интерфейсы управления и среды разработки приложений, которые, по их расчетам, должны обеспечить удобство, экономическую эффективность и устойчивость в облачной среде. Однако проведенное в 2021 г. исследование Uptime Institute Intelligence о частоте отключений облачных сервисов показало, что они не всегда достигают желаемого.

Кто отвечает за сбои в облаках? Пользователи, которые не смогли спроектировать устойчивые приложения, или облачные провайдеры, не обеспечившие надлежащее качество услуг? Чтобы ответить на этот вопрос, рассмотрим ключевые принципы облачных вычислений.

Устойчивость одиночного облака

Облако – модель, обеспечивающая повсеместный и удобный сетевой доступ по требованию к общему пулу настраиваемых вычислительных ресурсов. Основное преимущество облачных вычислений – масштабируемость, способность

быстро увеличивать или уменьшать объем ИТ-ресурсов по мере необходимости для удовлетворения меняющегося спроса.

Облачные ресурсы предоставляются пользователю как услуга. Пользователь выступает стороной, которая потребляет услуги, а также, как правило, несет расходы, связанные с их использованием. Поставщик (провайдер) – это сторона, управляющая (или отвечающая за управление) облачным сервисом, который может включать в себя ЦОД, физические серверы, сетевые устройства и ПО, задействованные для предоставления услуг.

Масштабируемость облачного приложения обеспечивается благодаря пяти свойствам облака:

- самообслуживание по требованию. Приложения могут получить ресурсы при необходимости, автоматически и без участия человека;
- универсальный доступ по сети. Приложения способны автоматически распределять трафик между ресурсами;
- объединение ресурсов. Приложения могут использовать общий пул однородных и взаимозаменяемых ресурсов; приложение не привязано постоянно к какому-либо определенному ресурсу;
- эластичность. Приложения могут увеличивать объем потребляемых ресурсов при необходимости;
- учет услуг. Доступ к дополнительным ресурсам обеспечивается провайдером, взимающим плату пропорционально их использованию.

В облачных вычислениях термин «приложение» означает используемые облачные службы, набор этих служб, а также пользовательский программный код, представляющие в совокупности ценность для пользователя. Рабочая нагрузка – это реально работающий ресурс приложения. Виртуальные машины, базы данных, контейнеры – примеры рабочих нагрузок, которые при правильной компоновке обеспечивают реализацию заявленных целей.

Масштабируемость приложения не сводится только к динамическому увеличению или умень-

шению объемов доступных ресурсов в соответствии с меняющимися требованиями, но предполагает задействование нескольких ЦОДов для обеспечения устойчивости. Устойчивость достигается за счет использования нескольких регионов и зон доступности.

Регион – это географическая область, содержащая набор зон доступности (логических дата-центров). Каждый регион физически изолирован от другого и независим от него в плане энергетических, сетевых и прочих ресурсов.

Зона доступности – это логический ЦОД или несколько ЦОДов в пределах региона. Обычно предполагается, что у каждой зоны имеются отдельное и резервированное электропитание и сетевые ресурсы. Одна зона доступности не обязательно состоит из одного дата-центра.

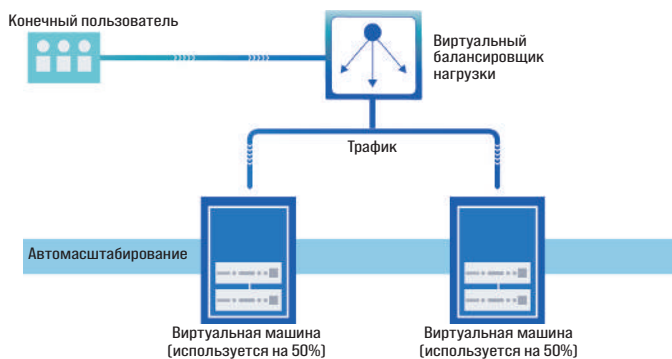
Гиперскейлеры, в том числе Amazon Web Services (AWS), Microsoft Azure, Alibaba Cloud, IBM Cloud и Google Cloud Platform, заранее предупреждают клиентов о возможности сбоев в пределах одной зоны доступности. Эталонная архитектура, предоставляемая этими провайдерами, определяет базовые конфигурации ресурсов, в число которых входит использование нескольких зон доступности для обеспечения устойчивости.

Однако гиперскейлеры не описывают детально необходимый уровень избыточности или профили риска для отдельных регионов или зон доступности. Они объясняют, как разработать приложение с отказоустойчивой архитектурой, но не могут четко сказать, какие уровни устойчивости будут при этом достигнуты.

Согласно проведенному в 2021 г. Uptime Institute Intelligence глобальному исследованию, лишь 18% владельцев и операторов ЦОДов считают, что располагают достаточной информацией об эксплуатационной устойчивости. При этом почти каждый четвертый заявляет, что более высокая информированность побудит их использовать облако для критически важных приложений.

Масштабируемость и отказоустойчивую архитектуру в облаке лучше всего описать на примере простого веб-приложения, развернутого у провайдера публичного облака (рис. 1).

Показанный на рис. 1 виртуальный балансировщик нагрузки работает по модели PaaS («Платформа как услуга»). В соответствии с этой моделью провайдер управляет ЦОДом, физическим сервером и промежуточным ПО (middleware), включая его распределение по нескольким зонам доступности и масштабирование с учетом изменяющихся требований, и отвечает за его функциональность. В нашем случае промежуточное ПО – это программный код, обеспечивающий работу балансировщика нагрузки. Пользователь может настраивать неко-



▲ Рис. 1. Простая облачная архитектура с балансировщиком нагрузки

торые компоненты такого ПО, но не может редактировать базовый код или получать доступ к серверу и ЦОДу.

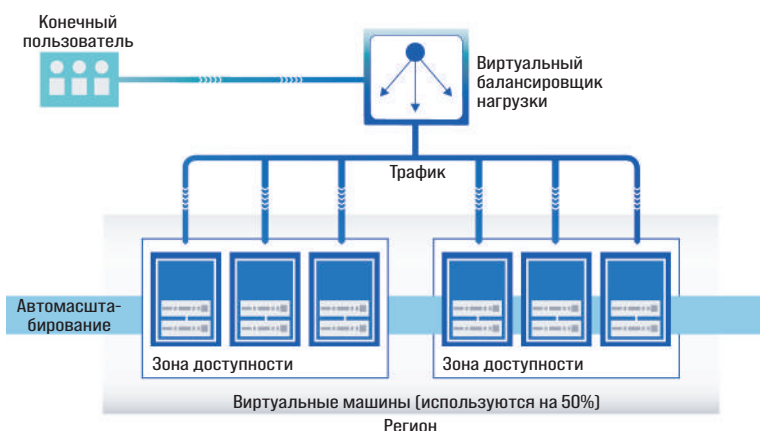
Трафик от конечных пользователей в интернете направляется в балансировщик нагрузки, который распределяет его между двумя виртуальными машинами. Они находятся в группе автоматического масштабирования, в рамках которой провайдер отслеживает загрузку центральных процессоров виртуальных машин. При достижении установленного порогового значения в группу автоматически добавляются дополнительные виртуальные машины и балансировщику нагрузки поступает информация о доступности новых мощностей.

У этой архитектуры уже есть некоторая устойчивость: если одна из виртуальных машин выходит из строя, группа масштабирования автоматически выявляет необходимость добавления емкости, и приложение масштабируется. Каждая виртуальная машина может работать независимо, оставаясь при этом частью одного приложения.

Для повышения отказоустойчивости виртуальные машины могут быть распределены между зонами доступности (рис. 2). В случае выхода из строя одной зоны доступности целиком группа масштабирования обнаружит необходимость добавления емкости, поэтому приложение останется работоспособным.

Виртуальные машины на обеих схемах работают по модели IaaS («Инфраструктура как услуга»). Это означает, что провайдер отвечает за

Рис. 2. Облачная архитектура с балансировщиком нагрузки между зонами доступности ▼



ЦОД, физический сервер и механизм разделения серверов на блоки, доступные по требованию, – обычно через виртуализацию. В зону его ответственности входят установка, обслуживание и обновление аппаратного и программного обеспечения для реализации согласованного с пользователем уровня предоставления услуг. У пользователя нет доступа к ЦОДу, серверам или уровню виртуализации. При этом он отвечает за масштабирование и устойчивость. Архитектура, показанная на рис. 2, разработана так, чтобы виртуальные машины были масштабируемыми и устойчивыми.

Как уже говорилось, балансировщик нагрузки и группа автомасштабирования работают по модели PaaS, поэтому за их масштабирование и устойчивость отвечает провайдер. Для эффективного управления балансировщиком (включая ЦОД, базовое оборудование и код самого балансировщика) при использовании сервисов PaaS пользователь должен доверять облачному провайдеру, который обязуется обрабатывать сигналы о повышении спроса и реагировать на перебои в работе должным образом.

Несмотря на то что пользователь для своего приложения спроектировал виртуальные машины с учетом масштабирования в нескольких зонах, если при сбое провайдеру не удастся задействовать службы автомасштабирования или балансировки нагрузки, приложение будет недоступно. Устойчивость прочих облачных сервисов, таких как базы данных, интерфейсы управления, службы хранения и шлюзы API, также обеспечивается облачным провайдером.

Довольно просто разработать приложение, которое кажется масштабируемым и отказоустойчивым, используя предоставляемые облачными провайдерами балансировщики нагрузки и зоны доступности. Однако оценить масштабируемость и устойчивость приложения количественно может быть сложно из-за того, что провайдер не предоставляет информацию о профилях риска базового ЦОДа, инфраструктуры и платформы.

Для повышения отказоустойчивости системы, показанной на рис. 2, трафик можно было бы распределять по нескольким регионам (с большей степенью разделения с точки зрения инфраструктуры ЦОДов), используя службы балансировки нагрузки на основе DNS. Такую архитектуру сложно и дорого проектировать из-за проблем с пропускной способностью: задержка между регионами может снизить производительность, а репликация данных между регионами – увеличить затраты на трафик. У пользователей как минимум должен быть резервный репозиторий кода и конфигураций, которые можно использовать для восстановления

приложения в другом облачном регионе в случае выхода из строя основного региона.

Альтернативные облачные провайдеры, такие как OVHcloud, Linode и DigitalOcean, в отличие от гиперскейлеров предлагают гораздо более ограниченный спектр услуг и вариантов настройки. Стандартизация и автоматизация снижают накладные расходы и соответственно цены. Ключ к успеху – простота: эти провайдеры уделяют больше внимания рекламе устойчивости своей инфраструктуры, а не предлагают клиентам самим создавать устойчивые приложения с балансировкой трафика между ЦОДами. Но они также располагают набором услуг для обеспечения масштабируемости, в числе которых балансировщики нагрузки, зоны доступности и автомасштабирование.

Гибридное облако и мультиоблако

На рынке все еще путают термины «гибридное облако» и «мультиоблако», и они часто используются как синонимы. Чтобы внести ясность, мы дадим простые определения. Гибридное облако – это одно публичное облако и одно частное облако, управляемые через единый интерфейс. Мультиоблако – это любое количество публичных и частных облаков, объединенных единым интерфейсом управления. На практике, впрочем, мультиоблако чаще ориентировано на то, чтобы приложения могли работать у конкурирующих провайдеров общедоступных облаков, а не с частными платформами.

Мультиоблако не очень практично

Учитывая отсутствие количественной информации от облачных провайдеров, подтверждающей отказоустойчивость, легко понять, почему некоторые пользователи предпочитают создавать приложения, работающие на нескольких облачных площадках. В принципе у каждого облачного провайдера должна быть своя инфраструктура ЦОДов – сбой у одного провайдера не должен влиять на другого. Однако в сдаваемых в аренду дата-центрах и в общих кампусах ЦОДов разные провайдеры довольно часто полагаются на одни и те же источники электропитания и воды и, кроме того, могут совместно использовать одни и те же сетевые ресурсы. Инциденты с любым из этих ресурсов повлияют на всех поставщиков.

Помимо повышения отказоустойчивости инфраструктуры использование нескольких облачных провайдеров повышает устойчивость с коммерческой и юридической точек зрения. От того, что поставщик облачных услуг прекратит свою деятельность или столкнется с юридическими проблемами, конкурирующий провайдер, скорее всего, не пострадает. Некоторые организации поддерживают отношения с не-

сколькими провайдерами и поэтому могут оказать на них давление, чтобы получить более привлекательные условия.

Главная проблема создания приложений в нескольких общедоступных облаках заключается в том, что инструменты, обеспечивающие масштабируемость и устойчивость, являются проприетарными и не могут взаимодействовать друг с другом – они эффективно работают только у того провайдера, который их разработал. Критический момент – несовместимость интерфейсов API. В облачных вычислениях разработчики ПО используют API для запросов к провайдеру, к примеру, для предоставления дополнительной емкости. Облачные провайдеры также применяют их для связи между сервисами. Так, группа автомасштабирования использует API для измерения загрузки центральных процессоров виртуальных машин.

Не составляет труда скопировать и вставить код, работающий на виртуальной машине в одном облаке, на виртуальную машину в другом, если операционная система на этих машинах одна и та же (обычно это Linux). Однако вспомогательные услуги PaaS, которые делают каждую услугу масштабируемой и устойчивой, скопировать затруднительно. Например, балансировщик нагрузки AWS создан только для внутреннего использования AWS, и его код недоступен для пользователей. Он использует API-интерфейсы AWS для связи с другими сервисами AWS и не может взаимодействовать с Microsoft Azure и Google Cloud.

Очень мало приложений способны работать у конкурирующих облачных провайдеров. Мультиоблачное приложение должно быть спроектировано так, чтобы оно могло использовать разные облачные API, каждый из которых имеет свои характеристики и возможности. Для каждого провайдера заказчику потребуются отдельные группы специалистов, включая разработчиков, архитекторов ПО и специалистов по безопасности, что в итоге увеличит затраты. Улаживание проблем между провайдерами также будет сложной задачей.

В настоящее время реальнее схема, когда в гибридном облаке один провайдер публичного облака будет работать с одним частным облаком, чем когда несколько разных площадок будут работать друг с другом.

Гибридное облако – это компромисс

Платформы управления облачными средами (Cloud management platform, CMP) предлагают стандартный графический интерфейс для управления как публичными, так и частными облачными площадками, взаимодействуя с ними с помощью соответствующих API. CMP мо-

гут также управлять ресурсами инфраструктуры, например, переместить виртуальную машину из одной среды в другую. Но они не могут переместить приложение от одного облачного провайдера к другому, потому что приложение, скорее всего, было создано с учетом особенностей конкретного провайдера.

Исторически CMP создавались компаниями – разработчиками ПО, такими как VMware, Turbonomic, IBM, Microsoft и ServiceNow. Не так давно гиперскейлеры начали поставлять локальные (on-premise) версии своих общедоступных облаков, обычно в виде сборки из серверов и СХД, устанавливаемых в ЦОДах клиента (два примера – AWS Outposts и Azure Stack Edge). Такие площадки функционируют как частные облака в том смысле, что услуги дата-центра здесь обеспечивает ИТ-отдел заказчика. Провайдер публичного облака отвечает за оборудование и промежуточное ПО, обеспечивающее облачную функциональность, и ИТ-отдел заказчика не может вносить в них какие-либо изменения.

Эти частные облака не предназначены для работы независимо от публичного облака. Их лучше всего рассматривать в качестве расширений публичного облака для локального ЦОДа, поскольку администрирование и обслуживание выполняются через публичное облако. Благодаря тому, что общедоступное и частное облака используют одну и ту же платформу и API, приложения можно создавать в разных местах: как в локальном дата-центре организации, так и в ЦОДе облачного провайдера, и платформа может управляться как единое целое. Часто организуется также выделенное сетевое соединение между публичным и частным облаками.

Устойчивость этой архитектуры не гарантируется, поскольку работа приложения по-прежнему зависит от способности облачного провайдера управлять некоторыми службами, в частности интерфейсом управления. Если этот интерфейс выйдет из строя, то пропадет возможность администрировать локальное облако. В этом случае пользователь все так же доверяет провайдеру обеспечение устойчивости балансировщиков нагрузки, групп автомасштабирования и других инструментов. Если сетевое соединение между публичным и частным облаком прервется, частное облако станет недоступным.

Согласно данным Uptime Institute Intelligence, даже с CMP и локальными облачными площадками 20% провайдеров считают управление различными площадками самой большой проблемой для своих клиентов, уступающей по значимости только прогнозированию будущих требований к емкости.

Несмотря на то что гибридной инфраструктурой можно управлять через единый интерфейс,

лишь немногие приложения работают в гибридных средах. Обычно частное облако используется для приложений с особыми требованиями к независимости или производительности. Общедоступное облако, напротив, применяется для front-end веб-серверов, пакетной обработки, средств тестирования и разработки. Основное преимущество интегрированного гибридного подхода заключается в том, что при необходимости пользователь может перемещать ресурсы между облаками. К примеру, если приложение из публичного облака нужно переместить в локальное частное облако из-за проблем с соблюдением каких-либо требований, то это можно сделать относительно быстро и легко (по сравнению с перемещением между облаками конкурирующих провайдеров) с помощью единого интерфейса, поскольку оба облака используют одни и те же API.

Часто эта гибкость добавляет руководителям уверенности: ИТ-директор понимает, что при необходимости приложение всегда можно вернуть обратно в локальный ЦОД организации. Другое важное преимущество гибридного облака заключается в том, что управление им осуществляется через единый интерфейс, пользователь получает единый счет и существует единая техподдержка.

Гибридный облачный подход – это компромисс: он предоставляет больше возможностей выбора места размещения рабочих нагрузок по сравнению с использованием только публичного облака, но с меньшим количеством площадок, чем мультиоблачный подход.

Контейнеры, микросервисы и облачно ориентированные инструменты

Виртуализация – это механизм одновременного запуска нескольких операционных систем на физическом сервере, часто с целью максимизации его загрузки. Уровень виртуализации (гипервизор) разделяет физические аппаратные ресурсы между несколькими виртуальными

машинами. Каждая виртуальная машина имеет свою ОС и выполняет программы в пределах выделенной доли аппаратных ресурсов.

Контейнеры

С программными контейнерами виртуализация делает шаг вперед: они совместно используют как физический сервер, так и ОС. В контейнере содержатся программный код и все библиотеки, необходимые для его исполнения. Логический механизм упаковки, реализованный в контейнерах, позволяет абстрагировать (изолировать) приложения от облачной среды, в которой они работают. Кроме того, код и библиотеки в контейнере абстрагируются и от ОС (рис. 3).

Контейнеризация

Движок контейнеризации, установленный в операционной системе на сервере, поддерживает работу с несколькими контейнерами. Каждый контейнер исполняет код рабочей нагрузки.

Существенное преимущество контейнеров перед виртуальными машинами заключается в том, что при необходимости расширения емкости для них не нужно устанавливать новую ОС. Легкий контейнер может существовать всего несколько секунд и потреблять ничтожную долю физических ресурсов (тем самым ощутимо снижая энергопотребление ИТ-инфраструктуры). Контейнер можно с легкостью перемещать с платформы на платформу, поскольку в нем содержится все необходимое для запуска в операционной системе. Поэтому контейнеры отличаются высокой переносимостью, масштабируемостью и эффективностью.

Микросервисы

В разделе «Устойчивость одиночного облака» мы обсуждали отделение кода от инфраструктуры путем распределения данных между рабочими нагрузками. Код можно также дополнительно разделить с помощью микросервисов. Микросервисная архитектура разбивает приложение на множество небольших функций, каждая из которых работает независимо, обычно в пределах контейнера. Как правило, микросервисы взаимодействуют друг с другом через API.

На рис. 4 показано, как немикросервисная архитектура масштабируется в ходе работы. В этом примере требованиям к производительности облачного приложения удовлетворяет одна виртуальная машина. В момент времени 0 достигается максимальная мощность виртуальной машины. Система автоматического масштабирования создает новую виртуальную машину для увеличения емкости, но это занимает около 5 мин, так как каждой виртуальной машине необходимо полностью загрузить ОС. Баланси-

Рис. 3. Компоненты виртуализации и контейнеризации ▼



ровщик нагрузки (не показан на схеме) распределяет данные по виртуальным машинам. При падении спроса дополнительная виртуальная машина может отключиться автоматически. Принятие решения об ее отключении осложняется тем, что для повторного запуска снова потребуется 5 мин, а слишком раннее отключение может привести к задержкам при повторном повышении спроса.

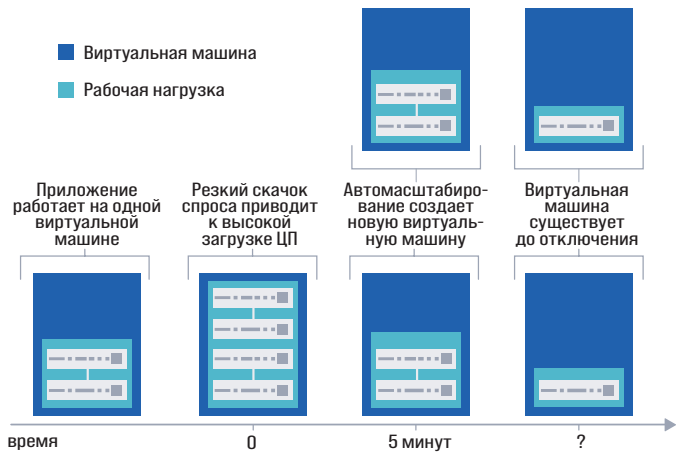
В микросервисной архитектуре (рис. 5) приложение разделено на два сервиса, А и В. Каждый сервис может создавать дополнительную емкость, добавляя контейнеры для управления нагрузкой.

В момент времени 0 достигается пороговое значение емкости виртуальной машины или сервера. Сервис А имеет достаточно ресурсов, но сервис В испытывает затруднения и снижает производительность приложения. Через 10 с приложение завершает работу контейнеров с сервисом А и отдает приоритет сервису В для временного удовлетворения потребности в емкости. Сервисы взаимодействуют друг с другом с помощью API. Завершив свои задачи, контейнеры закрываются, а новые контейнеры, поддерживающие сервис А, создаются через 20 с.

Облачно ориентированные технологии

Пример на рис. 5 иллюстрирует гибкость, которой позволяют добиться контейнеры. Приложение может реагировать на ежесекундные изменения спроса, разделяясь на отдельные компоненты, способные масштабироваться независимо друг от друга. В сложном приложении тысячи контейнеров могут работать на сотнях серверов, расположенных на нескольких площадках. Облачно ориентированные технологии – это набор инструментов, используемых для отслеживания микросервисов и их эффективной совместной работы. Docker – наиболее распространенный движок контейнеризации, который абстрагирует код от операционной системы. Платформа с открытым исходным кодом Kubernetes (она же K8s) – самое известное и чаще всего применяемое ПО для управления жизненным циклом контейнеров: оно автоматизирует развертывание, масштабирование и управление контейнеризованными приложениями.

Cloud Native Computing Foundation (CNCF), проект некоммерческой организации Linux Foundation, отслеживает свыше 1200 проектов, продуктов и компаний, связанных с облачно ориентированными технологиями. Цель CNCF – снизить сложность этих технологий. Но пока все они находятся в зачаточном состоянии, и не существует простого стандартного подхода к реализации облачно ориентированных концепций. Контейнеры и микросервисы, разбивая

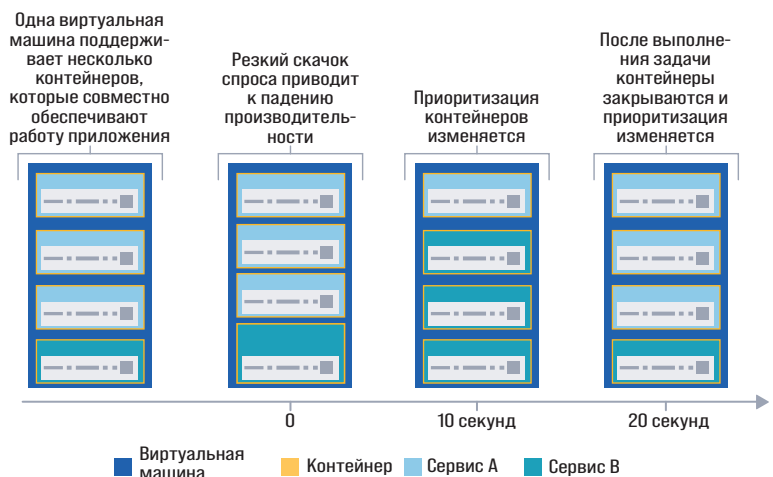


▲ Рис. 4. Создание виртуальных машин в немикросервисной архитектуре

приложения на большое количество частей, затрудняют их отслеживание и управление ими. Облачно ориентированные инструменты могут снизить техническую сложность, но само их внедрение – задача нелегкая.

Поскольку контейнеры легки, абстрагированы от оборудования и операционных систем и управляются через API, поставщики облачных услуг все чаще используют их для поддержки мультиоблачных сред. Google Anthos и Microsoft Azure Arc – это платформы управления контейнерами, работающие в публичных и частных облаках. Изначально эти платформы имели дело только с контейнерной службой своего провайдера, но сейчас они также могут управлять контейнерами в промежуточном ПО, установленном пользователем в локальной инфраструктуре и конкурирующих облачных сервисах. Такая модель может повысить устойчивость, помогая создавать приложения для разных облачных провайдеров и площадок. Однако сложность управления контейнерами и микросервисами может привести к другим проблемам, способным повлиять на устойчивость. Технология применения контейнеров для обеспечения устойчивости и масштабируемости в облаках все еще находится в стадии разработки.

Рис. 5. Создание контейнеров в микросервисной архитектуре ▼



Кто виноват и что делать

С укрупнением облачных провайдеров и усложнением их сервисов количество сбоев в работе облаков, по всей вероятности, возрастет. Увеличение числа систем, работающих на многих площадках, неизбежно приведет к большому числу отказов. По мере распространения облачных вычислений влияние этих сбоев, видимо, также будет расти, поскольку все больше пользователей полагаются на облачные вычисления для развертывания своих приложений.

Это возвращает нас к первоначальному вопросу: кто виноват в причинах сбоев? Ответ таков: облачный провайдер несет ответственность за работоспособность своих служб, но и пользователь должен создавать надежные приложения, чтобы они могли быстро восстанавливаться в случае сбоев. Облачные провайдеры, как правило, открыто говорят о том, что их инфраструктура иногда может выходить (и выходит) из строя.

Будут ли пользователи в ответ на свои создавать более устойчивые облачные архитектуры? Или же они продолжают обвинять облачных провайдеров либо вообще будут избегать публичных облаков? Организации вряд ли полностью откажутся от публичных облаков из-за таких преимуществ, как высокая масштабируемость, удобство и быстрый доступ к новым услугам. А давление на облачных провайдеров вряд ли приведет к успеху (если это не давление регулятора). Провайдеры пытаются сбалансировать функциональность, стоимость и производительность. Их цель не в том, чтобы обеспечить высочайшее качество по самой высокой цене; они стремятся предложить клиентам необходимую функциональность и хорошее соотношение цены и качества.

Облачный сервис – это сложная комбинация ЦОДа, аппаратного и программного обеспечения. Время от времени эти службы будут давать сбои из-за непредсказуемого поведения взаимодействующих систем и людей. Поэтому пользователи должны:

- взять на себя ответственность за разработку отказоустойчивых приложений с использованием инструментов и сервисов облачных провайдеров;
- принять тот факт, что, если вы отдаете часть своих ИТ-систем на аутсорсинг провайдеру, иногда дела могут пойти не так.

Конечно, сбои случаются, даже если инфраструктура полностью управляется собственными силами и находится в локальном ЦОДе организации. Необлачная среда не является идеально устойчивой. Принципиальное различие между облачными и локальными площадками заключается в том, что в последнем случае организация понимает уровень устойчивости, а в

первом – нет. Избыточность физического оборудования, использование защитных систем и четко регламентированные процессы управления и эксплуатации локального ЦОДа известны и могут отслеживаться. Могут проводиться оценки рисков и устойчивости, а также аудиты.

В облачных вычислениях инфраструктура скрыта от пользователя. Облачные провайдеры не любят обсуждать свои системы, опасаясь, что при этом они могут раскрыть проприетарные технологии. Это также побуждает потенциальных клиентов более пристально изучать деятельность провайдеров и критиковать их.

В результате роста числа отключений облачных сервисов пользователи, вероятно, не будут полагаться на услуги какого-либо одного облачного провайдера. Они будут придерживаться открытого подхода к платформам, площадкам и поставщикам и выбирать наилучшую среду для каждой отдельной рабочей нагрузки – мультиоблачную стратегию, но не обязательно интегрированную мультиоблачную платформу. Как только у организаций появятся навыки и намерение создавать устойчивые приложения, влияние сбоев, вероятно, уменьшится, но это займет время. Многие организации предпочтут оставить критически важные рабочие нагрузки в локальном ЦОДе, а не рисковать передачей управления облачному провайдеру. Но не многие организации полностью откажутся от облаков.

Сегодня большинство заказчиков осознают, что внедрение мультиоблачных сред для них слишком тяжелая задача. В обозримой перспективе большинство приложений будут работать с одним облачным провайдером. Они могут быть спроектированы так, чтобы использовать несколько зон или регионов доступности, но провайдер будет один. Многие пользователи придут к выводу, что удобство общедоступного облака стоит того, чтобы время от времени быть недоступным.

Гибридное облако, облачно ориентированные технологии и микросервисы до сих пор остаются новыми технологиями, и поэтому не существует стандартного подхода или архитектуры для их использования. При правильном применении они могут сделать приложения более устойчивыми, но также могут повысить сложность эксплуатации и создавать проблемы с производительностью и доступностью. До сих пор трудно оценить чистую выгоду от этих новых технологий, а их сложность, скорее всего, будет нарастать.





DATA CENTER DESIGN & ENGINEERING

10-я КОНФЕРЕНЦИЯ И ВЫСТАВКА

23 мая 2023

Москва.

Проектирование и строительство ЦОДов – важнейшие шаги создания цифровой инфраструктуры предприятий, регионов и страны в целом. Эффективность этих процессов во многом определяется экспертизой и наличием технологий в области инженерных систем и архитектуры как отдельных ЦОДов, так и территориально распределенных комплексов.

Сегодня рынок инженерных систем ЦОДов находится в стадии серьезной трансформации. Вслед за пандемией возникли новые вызовы, связанные с беспрецедентными санкциями. Но возникшие трудности не отменяют рост отрасли. Масштаб и количество крупных ЦОДов увеличиваются, активно создаются дата-центры в регионах.

Фокус DCDE-2023

- Отечественные решения для инженерной инфраструктуры ЦОДов
- Мини-/микроЦОДы для пограничных вычислений (Edge Computing)
- Охлаждение: от прецизионных кондиционеров к «холодным стенам»
- Новые подходы к обеспечению отказоустойчивости сети ЦОДов
- Искусственный интеллект и системы автоматизации в современном ЦОДе



dcdeforum.ru

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

16+

Реклама

ОРГАНИЗАТОРЫ

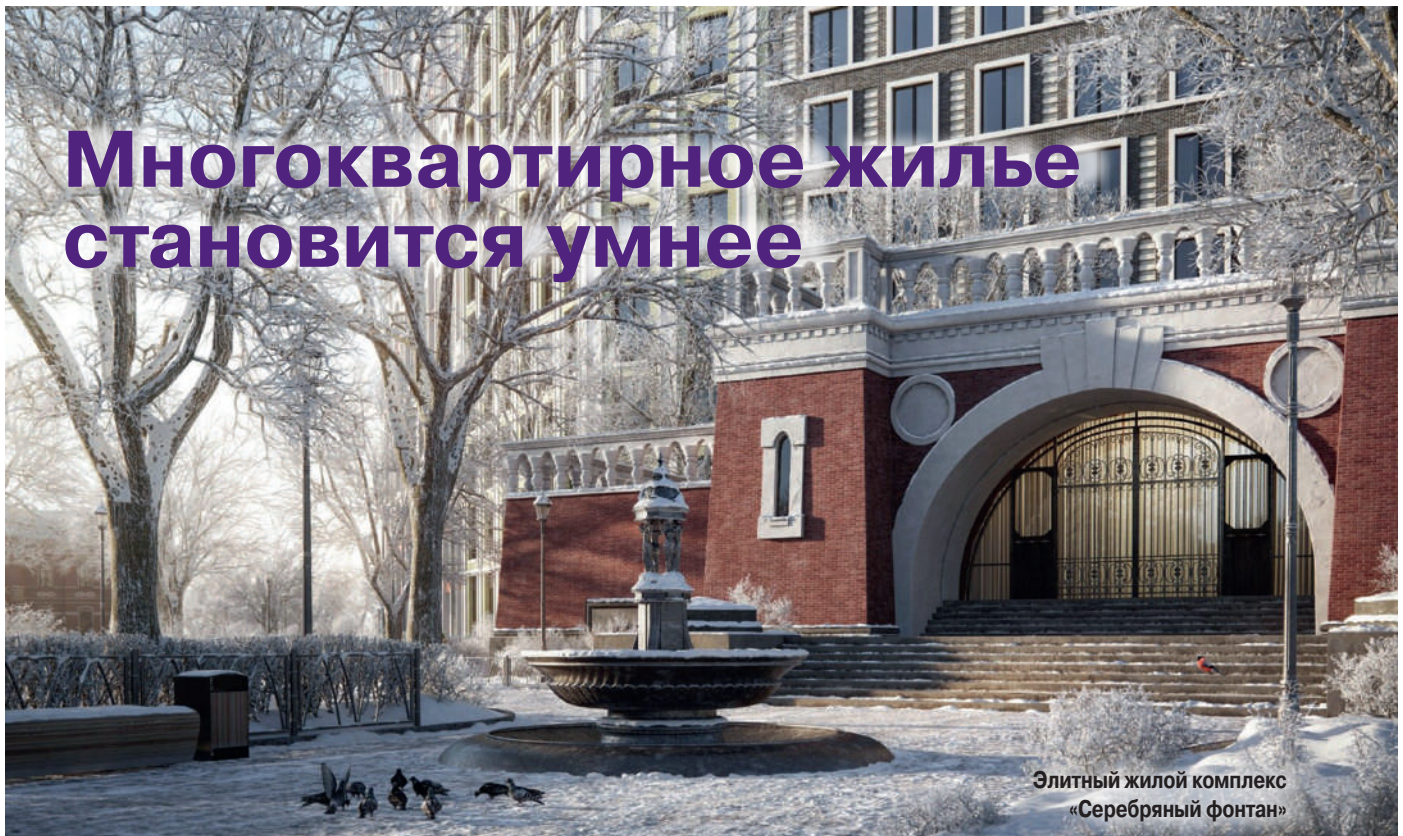


ПРИ
ПОДДЕРЖКЕ
И УЧАСТИИ



КООРДИНАЦИОННЫЙ СОВЕТ
ПО ЦОДАМ И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ
Автономная некоммерческая организация

Uptime Institute®



Многоквартирное жилье становится умнее

Элитный жилой комплекс
«Серебряный фонтан»

Николай
Носов

У строителей многоквартирных домов растет интерес к системам «умного» дома, повышающим энергоэффективность и престижность продаваемого жилья.

Престижная площадка и высокая готовность к использованию современных цифровых технологий – залог успеха на рынке недвижимости. Это поняла компания Sabey, создавшая в 2014 г. новый формат digital factory, объединяющий большие вычислительные мощности и престижные офисные площади на Манхэттене в Нью-Йорке. Российские маркетологи подхватили идею, и начали появляться цифровые здания, такие как «Голден Гейт» на Таганке – первый российский бизнес-центр, получивший сертификат цифровой недвижимости Cloud Ready Building Level 2. Проходят сертификацию и другие объекты, например, коворкинги Industrial City в Подмосковье.

Перспективна цифровизация и для рынка элитного жилья. Не все могут построить небоскреб на Манхэттене или домик с видом на Кремль, подчеркнуть свою элитность наличием в жилом комплексе яхт-клуба и маяка (ЖК «Алые паруса») или гольф-клуба (ЖК Woods Moscow). Элитность достигается близостью к центру, авторским дизайном зданий, хорошей экологией, закрытостью территории, повышенной безопасностью. Важное дополнение – развитая экосистема внутренних сервисов, базирующихся на цифровых технологиях.

Продавцы квартир «River Park Towers Кузнецкий» акцентируют внимание на всесезонных беседках-иглу с Wi-Fi в зонах отдыха жильцов на крышах небоскребов и открывающемся оттуда виде на Москва-Сити. Стандартом для элитных многоквартирных жилых домов стали охватывающая места общего пользования комплекса охранная система видеонаблюдения, СКУД, видеодомофоны, внутридомовые цифровые сервисы и широкополосный доступ в интернет.

Элитное жилье наиболее полно охвачено цифровыми технологиями. Как правило, в таких ЖК развернуты комплексные системы «умного» дома, включающие установки фильтрации воды, многоступенчатые системы очистки и увлажнения воздуха, вакуумные системы мусороудаления, IP-домофонию и прочие повышающие комфорт и безопасность сервисы. Но они используются и в менее дорогой недвижимости классов «бизнес», «комфорт» и даже «эконом». Правда, уровень цифровизации непосредственно зависит от класса жилья. Так, если эконом-класс ограничивается системами безопасности (домофон и камера видеонаблюдения), то в комфорт-классе появляются отдельные решения, связанные с

кондиционированием, поддержанием температурного режима зданий, приточной вентиляцией, мониторингом инженерных сетей. Все чаще применяются системы интеллектуального учета использования ресурсов, которые стали обязательными для установки в новостройках в 2021 г.

Жилье бизнес-класса дополнительно оснащается слаботочными розетками, датчиками движения, моторизованными карнизами, запорной арматурой для воды и системой контроля протечек, системами управления климатом (теплыми полами, отоплением, кондиционированием) и видеонаблюдения (за местами общего пользования и квартирой), а также мультирум-системой, которая предназначена для перераспределения и передачи видео/аудиосигнала от источника к телевизору и динамикам, находящимся в разных частях квартиры или дома.

Наличия дата-центра в непосредственной близости даже от элитного ЖК не требуется. Как правило, для обработки основного объема информации хватает edge-устройств и пары серверов в офисе управляющей компании. А облако используется для передачи данных с датчиков и устройств интернета вещей внешним поставщикам, например энергосбытовым или газовым компаниям, и для связи с мобильными устройствами жильцов. При этом цифровизация становится дополнительным элементом повышения престижности площадки, особенно в глазах молодого поколения, не представляющего жизни без смартфона.

Основные тенденции рынка «умной» недвижимости

Объем мирового рынка «умной» недвижимости постоянно растет. По данным Fortune Business Insights, в 2021 г. он оценивался в \$67,6 млрд, а к 2026-му, как ожидается, увеличится до \$177,8 млрд, при этом совокупный годовой темп роста составит 22,2% (рис. 1).

Драйверами развития рынка эксперты считают пандемию COVID-19, заставившую больше внимания уделять вопросам безопасности, и стремление использовать более энергоэффективные решения, снижающие вклад в глобальное потепление. Ведь, согласно исследованию Schneider Electric, 36% углеродных выбросов приходится на здания. Помимо экологической составляющей, высокое потребление энергии значительно увеличивает общую стоимость эксплуатации и обслуживания зданий, особенно в свете сегодняшнего роста цен на энергоносители, обусловленного геополитическими изменениями.

Внедрение «умных» технологий с использованием ИИ и IoT, по данным IBM, способно снизить потребление энергии на 40% и на 10–30% умень-

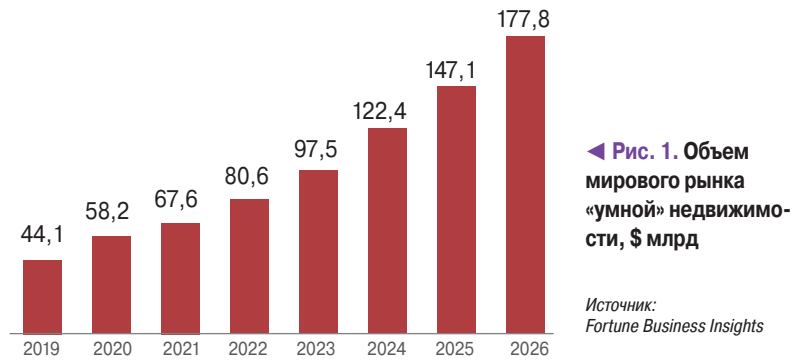


Рис. 1. Объем мирового рынка «умной» недвижимости, \$ млрд

Источник: Fortune Business Insights

шить затраты на техническое обслуживание. А в отчете Deloitte указывается, что внедрение «умных» технологий и устройств IoT позволило в некоторых проектах за три года уменьшить энергопотребление на 70%. Так что стремление к энергосбережению будет способствовать проникновению IoT на рынок недвижимости.

Сдерживающим фактором выступает рост числа кибератак. По данным аналитиков «Лаборатории Касперского», такому риску подвержены четыре из 10 «умных» зданий. Взлом системы даст возможность злоумышленнику контролировать перемещения жильца по общедомовой территории, открыть дверь его квартиры, восстановить точный распорядок дня – когда проснулся, что заказывал в интернете, какие телевизионные каналы смотрел. Не говоря уже о персональных данных – даже сам факт владения человеком элитной недвижимостью может использоваться для преступных действий.

Российский рынок

Рынок «умного» жилья в нашей стране также становится все более привлекательным для инвесторов. По данным МТС, в 2021 г. его объем составил 29,4 млрд руб., а в 2025 г. достигнет 95,6 млрд руб. (рис. 2).

Процессы цифровизации поддерживаются на государственном уровне. Согласно Федеральному закону от 27.12.2018 № 522, «многоквартирные дома, вводимые в эксплуатацию после осуществления строительства, должны быть оснащены... приборами учета электрической энергии, которые обеспечивают возможность их

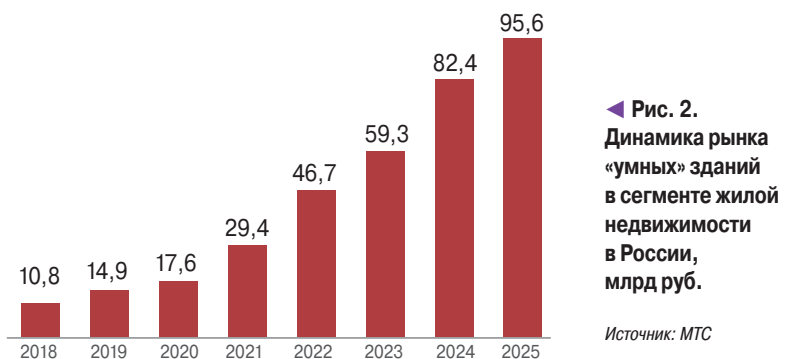


Рис. 2. Динамика рынка «умных» зданий в сегменте жилой недвижимости в России, млрд руб.

Источник: МТС

присоединения к интеллектуальным системам учета электрической энергии». То есть в новостройках счетчики в системе сбора данных об использовании электроэнергии уже должны быть немного «умными». Для того чтобы жильцам не нужно было отслеживать период подачи сведений о потреблении ресурсов, остается установить счетчики воды и газа, способные передавать собранные данные, а затем связать их с цифровой платформой.

Застройщикам цифровизация выгодна. При внедрении умной инфраструктуры себестоимость квадратного метра жилья увеличивается ненамного, но значительно повышаются его комфортность и престижность. Появляется вау-фактор, способствующий продаже. Кроме того, для управляющих компаний такая инфраструктура привлекательна благодаря тому, что она позволяет привязать жильцов за счет предоставляемых сервисов и дает возможность заработать на дополнительных услугах.

Строительные компании не имеют компетенций в области информационных технологий, поэтому для работ, связанных с цифровизацией зданий, привлекают интеграторов, в качестве которых зачастую выступают операторы связи. Последние свой главный козырь – опыт в области связи – дополняют экспертизой в проектировании и развертывании ИТ-систем, предоставляя заказчикам комплексное решение.

«Мы знаем, как увязать в умную цифровую инфраструктуру все, что нужно для застройщика. Благодаря модульности продукта заказчики выбирают только нужные приложения. Для каждого собирается индивидуальный набор сервисов на единой цифровой платформе», – дал комментарий нашему изданию руководитель стратегии IoT и промышленной автоматизации МТС Антон Салов.

Примером комплексного проекта может служить ЖК «Серебряный фонтан». На единой

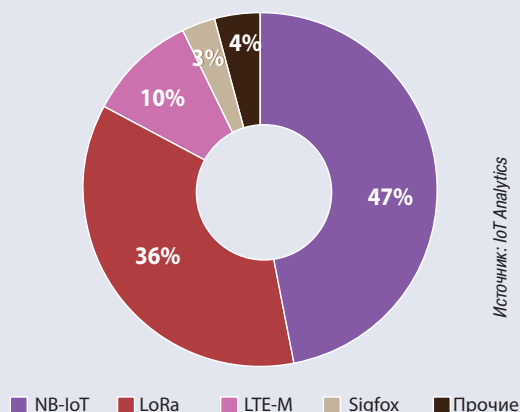
цифровой платформе развернуты системы контроля доступа и видеодомофоны, причем житель может увидеть посетителя через мобильное приложение в любой точке планеты. При приближении жильца «умные» двери открываются, реагируя на его смартфон, а «умный» лифт не только ждет посетителя, но и автоматически поднимает его на нужный этаж. Полезная функция для последователей религии, запрещающей в определенные дни любую работу, в том числе нажатие кнопок лифта.

Для развертывания ИТ-инфраструктуры требуется минимум проводов – площадь жилого комплекса покрыта сетью беспроводной связи стандарта NB-IoT. Благодаря высокой энергоэффективности батарейки в устройствах меняют редко: раз в шесть-десять лет. Показания датчиков и счетчиков видит обслуживающая (управляющая) компания, энергосбытовые компании и сам житель в приложении. Диспетчер управляющей компании получает изображения с видеокамер ЖК, отслеживает исполнение заявок жильцов, сигналы с датчиков, показания счетчиков и состояние выставленных счетов (рис. 3).

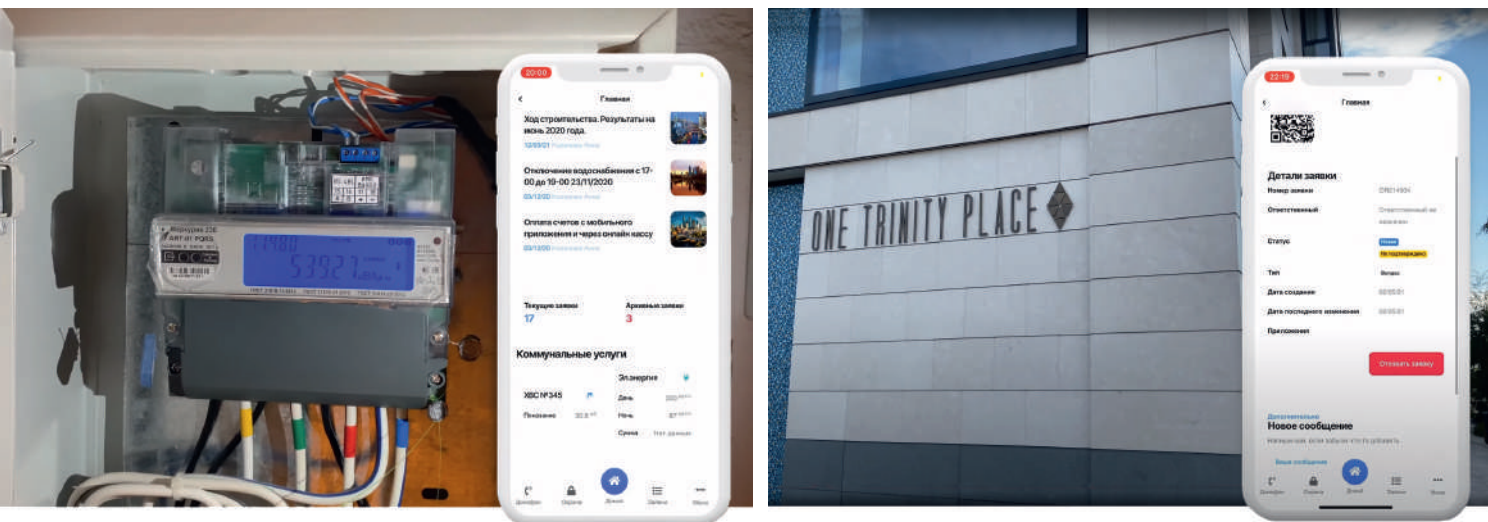
Заявки жильцов, например на уборку мусора, ликвидацию засора или замену перегоревшей лампочки на лестничной клетке, через приложение в смартфоне поступают в цифровую платформу. В едином информационном поле оказываются показания счетчиков, датчиков задымления и протечки воды, заявки на пропуск через ворота ЖК автотранспорта, данные о платежах. На базе цифровой платформы управляющая компания предоставляет дополнительные услуги, скажем, вывоз негабаритного и строительного мусора, ремонтные работы в квартире, разработку и согласование перепланировки и проектов инженерных систем. В случае нештатных ситуаций – срабатывания в квартире датчика движения, задымления, протечки воды – информация поступает в диспет-

▼ Рис. 3. В диспетчерской ЖК «Серебряный фонтан»

▼ ► Рис. 4. Структура LPWAN-подключений, 2021



Источник: IoT Analytics



Источник: Intelvision

черскую и непосредственно на мобильное устройство жильца. Диспетчер принимает меры – вызывает пожарных, наряд полиции или перекрывает подачу воды в квартиру.

Архитектура и технологии

В решении МТС не нужно разворачивать дополнительную инфраструктуру для подключения устройств – поддержку протокола NB-IoT обеспечивают существующие базовые станции компании. Стандарт сотовой связи NB-IoT популярен в мире. По данным GSMA, к марту 2022 г. в коммерческую эксплуатацию было запущено 110 таких сетей. Согласно IoT Analytics, на долю NB-IoT в 2021 г. приходилось 47% беспроводных LPWAN-подключений устройств интернета вещей в мире (рис. 4). Значительная часть внедрений приходится на Китай, где основными областями применения технологии стали учет водоснабжения и газа, обнаружение дыма и прокат велосипедов. Другая технология, LoRa, немного уступает по числу подключений (36%), но лидирует по распространению в мире (по данным LoRa Alliance, она используется в 170 странах).

В России технологию LoRa использует компания Intelvision, реализовавшая концепцию «умного» жилого комплекса в ЖК Miras Park и Dostyk Residence в Алматы. В работе находятся ЖК «Парад планет» в Москве и «Сосновый бор» в Санкт-Петербурге. Системами «умного» дома жильцы могут управлять через приложение на смартфоне (рис. 5) или установленный в квартире IP-домофон. Мобильное приложение позволяет передавать показания приборов учета ресурсов ЖКХ и проводить их онлайн-оплату, вести видеонаблюдение за квартирой, осуществлять контроль протечек, заказывать временные пропуска на территорию ЖК для посетителей и автотранспорта, ставить квартиру на охрану и снимать с охраны, заказывать различные услуги (ремонт, доставку еды и пр.).

Также доступны чат с управляющей компанией и новости ЖКХ и управляющей компании. Еще одно интересное решение – «умный» паркинг, включающий оптимальную организацию парковки, управление временем парковки, удобный поиск парковочных мест, «умное» освещение, RFID- и видеоидентификацию. Для набирающих популярность электромобилей предусмотрены AC/DC-зарядные станции.

Менее распространены сети на базе технологии Sigfox, используемые в 75 странах, большая часть из которых находится в Европе. Драйвером спроса на услуги LTE-M является прекращение предоставления услуг 2G в Северной Америке, Европе и некоторых странах Азиатско-Тихоокеанского региона. Технология LTE-M в основном задействуется для мониторинга промышленного оборудования.

По проводной и беспроводной связи первичные данные собираются и обрабатываются на месте, а более высокоуровневая обработка происходит в облаке. Например, данные ЖК «Серебряный фонтан» обрабатываются в ЦОДе МТС «Авантаж» в подмосковном Лыткарино.

Как сообщил А. Салов, на уровне рабочей группы при Минцифры России и АНО «Умный многоквартирный дом» разрабатывается концепция «умного» многоквартирного здания, которая предполагает использование для таких зданий edge-архитектуры. В ЖК выделяется специальное помещение для установки оборудования edge-платформы, управляющей автоматизированной системой жизнеобеспечения здания. «Самая правильная архитектура для «умного» здания – это edge», – считает А. Салов.

По оценке МТС, несмотря на рост интереса к системам «умного» дома со стороны застройщиков, доля новостроек, в проекты которых закладываются такие решения, пока не превышает 5%. Так что потенциал для дальнейшего роста есть. ИКС

▲ Рис. 5. Использование мобильного приложения для управления системами «умного» дома

Шпаргалки для киберкомиссаров

Николай Носов

Разработка отраслевых шаблонов оценки киберрисков поможет повысить защищенность российских предприятий.



Изменение ландшафта угроз

Конфликт на Украине привел к резкому увеличению количества кибератак на российские предприятия. Причем зачастую атакующие – это люди с низкой квалификацией, примыкающие к более профессиональным киберпреступникам. «Мы видим киберфольксштурм, которому раздали инструменты. Они ничего не понимают, но у них есть инструкция, и они по ней действуют», – так на онлайн-конференции AM Live+, посвященной управлению рисками информационной безопасности, объяснила рост числа атакующих Юлия Воронова, директор по консалтингу Positive Technologies. Интенсивность атак также повысилась. К внешним злоумышленникам все чаще добавляются инсайдеры, что, по мнению эксперта по исследованиям угроз информационной безопасности Центра исследования безопасности промышленных систем «Лаборатории Касперского» Владимира Дашенко, меняет ландшафт угроз.

Появились и «черные лебеди» – события, которые до того, как они произошли, казались почти невозможными. Так, если уход с российского рынка иностранных вендоров, в том числе тех, которые поставляют оборудование для систем информационной безопасности, еще можно было заложить в модель угроз, то сознательное внедрение в продукты open source вредоносного для определенных стран кода, – это, как считает Марат Цихмистров, руководитель направления консалтинга по информационной безопасности ГК Innostage, классический «черный лебедь».

На повестке дня – кибервыживаемость

Изменилась ситуация, изменились и угрозы и вероятности их реализации. Компаниям необходимо обновить модель угроз и риск-профиль, и руководство должно быть готово принять новые риски или предпринять шаги по их нейтрализации. Однако даже среди участников конфе-

ренции лишь 40% пересмотрели риск-профиль своей организации (рис. 1).

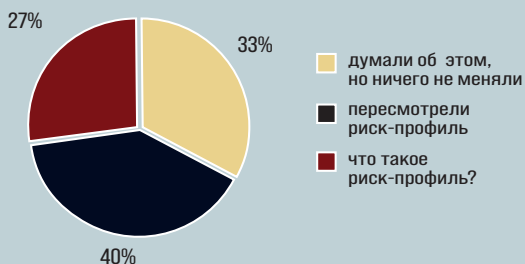
При этом главным риском кибербезопасности слушатели сочли остановку бизнес-процессов (рис. 2).

Остановка бизнес-процессов ставит под угрозу само существование бизнеса. «Никто не отменяет управление рисками и необходимость оценки вероятности событий, но шаг ноль – выявление недопустимых событий, приводящих к критичным для функционирования бизнеса последствиям, и защита от них. Это базовый уровень информационной безопасности. Сейчас надо сосредоточиться на кибервыживаемости – защите от недопустимых событий», – заявила Ю. Воронова.

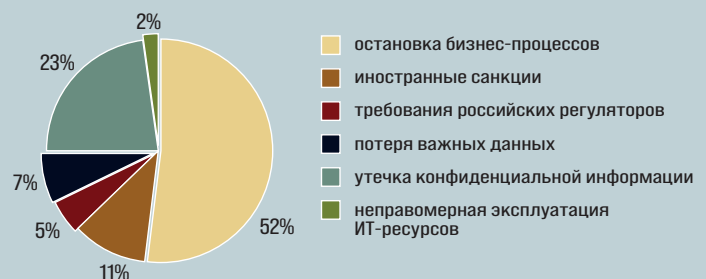
«Наша основная задача – не просто дать бизнесу выжить, а помочь стабильно и устойчиво работать и развиваться», – возразил М. Цихмистров. По мнению эксперта, лучше говорить не о кибервыживаемости, а о киберустойчивости. Да и киберриски – это не только риски информационной безопасности.

«С точки зрения управления рисками кибервыживаемость – частный случай. Возможно, в будущем мы придем от классического управления рисками к кибервыживаемости. Но большая часть компаний придерживается классического подхода, когда оцениваются не только критичные бизнес-процессы, а безопасность всех активов», – уверен В. Дашенко.

Нужно принимать во внимание цену вопроса. Если стоимость внедрения системы информационной безопасности больше, чем потери от нейтрализуемых угроз, то незачем тратить на нее ресурсы, разумнее риски принять. Но не следует впадать и в другую крайность – защищать только жизненно важные процессы и системы, а для остальных установить высокий приемлемый

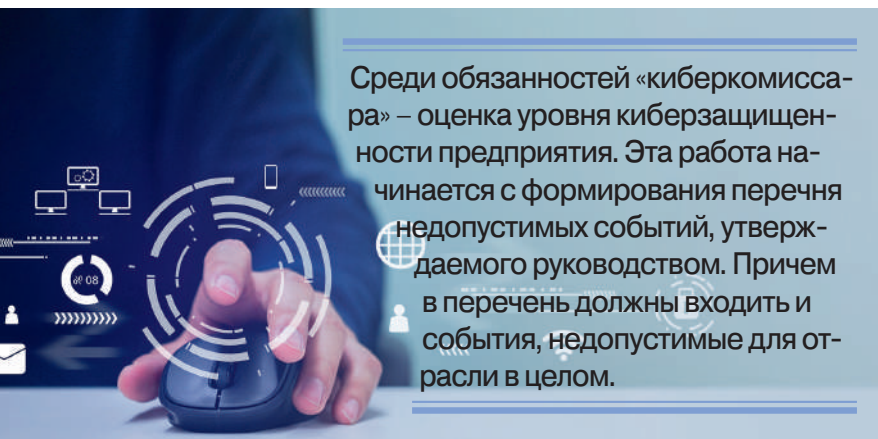


▲ Рис. 1. Пересматривали ли вы риск-профиль вашей организации после февральских событий?



▲ Рис. 2. Каков главный риск для вашей организации в 2022 г.?

Источник: Anti-Malware



Среди обязанностей «киберкомиссара» – оценка уровня киберзащищенности предприятия. Эта работа начинается с формирования перечня недопустимых событий, утверждаемого руководством. Причем в перечень должны входить и события, недопустимые для отрасли в целом.

уровень потерь и ничего не делать для нейтрализации угроз, несущих меньшие убытки. Если есть недорогие системы защиты, развертывание которых обойдется намного дешевле, чем ликвидация последствий реализовавшихся операционных и репутационных угроз, то их целесообразно установить.

Нужны отраслевые шаблоны

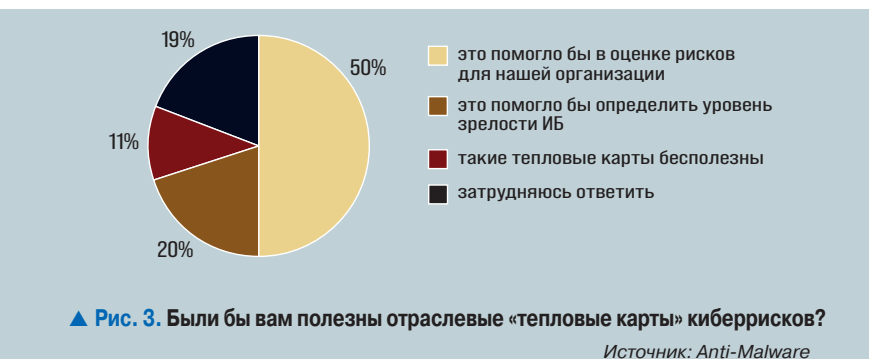
Если риски для отрасли в целом должны оцениваться независимыми структурами или регулятором, то важность рисков для конкретного предприятия определяет его руководство. Государство заниматься этим не может и не должно. Критичные для бизнеса события должно назвать высшее звено руководства – руководитель предприятия или его заместитель, на которого, согласно Приказу Президента РФ № 250, возложена ответственность за информационную безопасность организации. Среди обязанностей «киберкомиссара» – оценка уровня киберзащищенности предприятия. Эта работа начинается с формирования перечня недопустимых событий, утверждаемого руководством. Причем в перечень должны входить и события, недопустимые для отрасли в целом. «Надо выделить две категории – риски для предприятия и риски для отрасли как части государства. Есть вещи важные для государства, которые повлекут риски функционирования отрасли и жизнедеятельности граждан», – отметила Ю. Воронова.

В выборе направлений защиты руководители компаний могут опереться на создаваемые отраслевые шаблоны («тепловые карты» киберрисков) с перечнем угроз и численной оценкой вероятности их реализации на предприятиях отрасли. Такую карту использует, в частности, американская компания Cowbell для страхования киберрисков предприятий. В ее перечень угроз вошли: атаки на сетевую и облачную инфраструктуру, на финансовые транзакции, кибервымогательство и т.д. Например, для горнодобывающей промышленности, по мнению Cowbell, наибольшие риски представляют атаки на цепочки поставок, и компаниям отрасли особое внимание стоит уделять защите именно от этих угроз. Наиболее подверженными угрозам ожидаемо оказались финансовая отрасль и страхование: соответственно за страховку от киберинцидентов с финансовых предприятий стоит брать больше.

Разработка тепловых карт киберрисков ведется и в России. Между тем Евгений Сачков, эксперт по управлению рисками компании «Информзащита», к оценке вероятности недопустимых событий отнесся скептически, указав, что такие события зависят не только от отрасли, но и от популярности компании, ее активности в медийном поле, проработанности системы защиты и т.п. По его мнению, оценивать риски для конкретной компании следует с помощью не обобщенных тепловых карт, а специальных систем на основе факторного анализа для статистического моделирования и оценки ущерба в денежном эквиваленте. Однако большинство слушателей с этим не согласилось. Половина опрошенных сочла, что отраслевые тепловые карты киберрисков помогли бы оценить риски их организаций, по крайней мере в первом приближении (рис. 3). Ведь не все компании имеют соответствующую экспертизу и могут провести более точный анализ.

Для оценки существующих угроз, добавил В. Дащенко, также необходимо отслеживать информацию государственных, отраслевых и коммерческих центров реагирования на инциденты безопасности (CERT), предупреждающих о повышенных рисках атак на отдельные отрасли и их типах.

Но в главном все эксперты единодушны – нельзя ограничиваться «бумажной» безопасностью, выпуском и согласованием документов, важных для регулятора и для понимания ситуации с кибербезопасностью внутри предприятия. Нужно не просто оценить риски и составить нужные бумаги, а на основании проведенного анализа принять конкретные организационно-технические меры, направленные на их снижение. ИКС



Остановить телефонных мошенников

Число киберпреступлений растет. Для того чтобы справиться с ними, нужны совместные усилия финансовых организаций и правоохранительных органов – создание единой антифрод-системы на уровне страны.

Чем выше уровень цифровизации, тем активнее цифровые технологии задействуются для совершения преступлений. Атаки в основном идут из-за рубежа, и их количество постоянно растет. Играет свою роль и безнаказанность – в сложной геополитической ситуации атаки на российских граждан не только не несут никаких юридических рисков, но могут скрыто поощряться, рассматриваться как элемент необъявленной кибервойны. Лишь в феврале, сразу после начала СВО, число звонков из мошеннических колл-центров, по данным директора по противодействию мошенничеству компании Vi.zone Антона Окошкина, значительно снизилось. Впрочем, преступники быстро перестроились, и к настоящему времени, по оценкам руководителя бизнес-подразделения по противодействию мошенничеству Group-IB Павла Крылова, число атак по сравнению с прошлым годом увеличилось вдвое.

Массовое явление

Согласно выпущенному Банком России обзору операций, совершенных без согласия клиентов финансовых организаций за 2021 г., количество таких операций по переводу денежных средств увеличилось на 33,8% (1035,01 тыс. операций в 2021 г. по сравнению с 773,27 тыс. операций в 2020 г.). Объем операций также вырос на треть – до 13 582,23 млн руб. (9783,13 млн руб. в 2020 г.).

А в обзоре отчетности об инцидентах информационной безопасности при переводе денежных средств Банк России сообщил, что во II квартале 2022 г. выявлено 75 875 мошеннических мобильных телефонных номеров – рост на 2296,6% по сравнению со II кварталом 2021 г. (3166 номеров). На 33% увеличилось количество мошеннических номеров, начинающихся с

цифр 8-800, на 389,5% – городских номеров. А вот доля возмещенных средств в объеме украденных снизилась с 7,4% во II квартале 2021 г. до 5% в 2022 г.

По-прежнему у преступников популярны атаки с использованием социальной инженерии, на которые, по данным Банка России, стабильно приходится около половины (49,4%) операций без согласия клиентов. Тревожный новостной фон – отличная ситуация для мошенников, задача которых состоит в том, чтобы отключить аналитические способности человека, введя его в состояние стресса. Если собеседник все же сохраняет спокойствие, то стресс вызывают, сообщая ему, что у него воруют деньги или что близкий человек попал в аварию. Особенно гнусно выглядит обман стариков, которые зачастую совершенно беспомощны перед манипуляторами. А поскольку они сами снимают деньги со своих счетов и перечисляют их мошенникам, банки не несут ответственности за потери.

Всероссийский антифрод

Для выявления мошеннических операций банки используют разнообразные антифрод-системы, представляющие собой базу данных с правилами. Их можно разделить на две группы:

- транзакционные, которые анализируют параметры перевода денег, например, типичность операции и адресат получателя;
- ситуационные, анализирующие взаимодействие пользователя с фронт-системами банка, например, типичность его действий, геолокация, используемое устройство и возможность удаленного управления им злоумышленниками.

Но в случае использования социальной инженерии такая система малоэффективна, тем более когда обманутый человек сам приходит в

Николай Носов

банк. Здесь могут помочь и часто помогают операционисты, интересующиеся, зачем человек, особенно преклонного возраста, неожиданно снимает со счета все свои деньги. Они могут попросить прийти еще раз, чтобы подготовить заказанную сумму, но по большому счету не имеют права не выполнить требования клиента.

Финансовая система многогранна. Украденные деньги проходят по ней определенный путь, почти всегда для заметания следов переводятся в другие финансовые институты. Сейчас это проблема банка, с чьих счетов пытаются украсть деньги. Пока нет четкого понимания, как поступать его сотрудникам, как остановить мошенническую транзакцию в случае, когда обманутый человек осознал проблему. Конечно, есть законодательство об отмывании денежных средств, но небольшие суммы «под радары» подразделения финансового мониторинга не попадают.

Есть юридические сложности и в ведении базы дропперов – мошенников, обналичивающих украденные деньги. С одной стороны, внесение человека в черные списки без решения суда выглядит незаконным и создает большое поле для злоупотреблений. Да и не выдать деньги, ссылаясь на эти списки, банки не могут – в лучшем случае могут задержать под надуманным предлогом выдачу, ожидая запроса на отзыв мошеннической транзакции. С другой стороны, это последний рубеж, на котором еще можно спасти деньги клиента.

Эксперты не раз отмечали, что борьба с этим видом преступлений должна быть комплексной. В расследовании должна участвовать вся цепочка используемых мошенниками банков, от первого, где обманутый гражданин снимает свои сбережения, до банка, в котором дропперы обналичивают средства для преступников. Высказывались предложения усилить контроль за средствами, поступающими в банки. Контроль на всех этапах движения средств повысит возможности антифрод-систем банков, объединит отдельные базы с правилами в огромный «мега-антифрод» в масштабах страны.

Меры принимаются

30 декабря 2021 г. президент РФ подписал закон о введении административных штрафов за пропуск звонков с подменных номеров, которыми обычно пользуются мошенники. Причем наказание предусмотрено за каждый факт звонка, поступившего абоненту с такого номера. В августе 2022 г. российский суд впервые оштрафовал оператора связи за пропуск вызова с подменного номера от иностранного оператора. Штраф в 1 млн руб. наложили на компанию «Оранж Бизнес Сервисез», представляющую в России интересы телеком-концерна Orange Business Services.

Минцифры России подготовило проект правительственного постановления, согласно которому находящийся в ведении Роскомнадзора Главный радиочастотный центр (ГРЧЦ) становится оператором системы мониторинга блокировки звонков с подменных номеров. Операторы связи должны будут автоматически предоставлять системе сведения о звонках, включая их время и маршруты по сетям. Дополнительно будет необходимо устанавливать на сетях узлы верификации, предоставляемые ГРЧЦ. Однако центр еще не приступал к разработке системы, часть ее будет создана в текущем году. Тем временем критики проекта указывают на дополнительные затраты, которые будут вынуждены нести операторы связи, неэффективность при блокировке подменных звонков из-за рубежа и возможный скрытый саботаж со стороны мелких операторов, зарабатывающих на услугах предоставления подменных номеров.

18 октября нынешнего года Госдума в третьем чтении приняла поправки к законам «О банках и банковской деятельности» и «О национальной платежной системе». Согласно этим поправкам, Банк России будет предоставлять МВД «информацию, содержащуюся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента», на основании полученных от МВД сведений о совершенных противоправных действиях. 19 октября поправки одобрил Совет Федерации.

Теперь Банк России сможет быстро предоставить информацию обо всей цепочке транзакций, что станет основой для проведения оперативно-розыскных мероприятий. «Документ создает правовую основу для цифрового взаимодействия органов МВД и Банка России, который будет формировать базу данных по дропперам, занимающимся списанием средств со счетов», – отметил глава Комитета Госдумы по финансовому рынку Анатолий Аксаков.

В пояснительной записке к законопроекту предлагается осуществлять оперативный информационный обмен посредством технологической инфраструктуры Банка России – автоматизированной системы обработки инцидентов ФинЦЕРТ. Порядок информационного обмена, форма и перечень предоставляемых сторонами сведений будут закреплены в соглашении, которое заключат МВД и Банк России. Многие будут зависеть от конкретных деталей этого соглашения. Сейчас банки имеют право рассматривать обращения из полиции в срок до 30 дней, что существенно снижает раскрываемость преступлений.

Закон вступит в силу через год, в течение которого Банку России и МВД необходимо заключить соглашение и отработать информационно-техническое взаимодействие. **ИКС**



Мобильный ЦОД

ГК РСК представила мобильный ЦОД — разработку, которая способна обеспечить высокую вычислительную мощность, эффективную обработку и хранение данных даже в условиях полного отсутствия инженерной инфраструктуры.

Система отличается автономностью, легкостью конфигурирования, мобильностью, быстротой ввода в эксплуатацию и может быть развернута фактически в полевых условиях (в автомобиле, палатке, под навесом от осадков и т.д.) силами двух-трех человек за несколько десятков минут. Перевод из транспортного в рабочее состояние и обратно осуществляется без применения специализированного инструмента и/или технических средств.

Основу вычислительных мощностей мобильного ЦОДа составляет интероперабельная платформа на базе серверов «РСК Торнадо», которые позволяют использовать как отечественные, так и зарубежные процессорные архитектуры (x86, «Эльбрус» и др.). В нем применяется запатентованная технология жидкостного охлаждения РСК, что существенно повышает компактность и энергоэффективность. Для решения не требуется внешних инженерных подсистем. Возможно питание от мобильной электрогенераторной установки.

Мобильный ЦОД предназначен для периферийных вычислений и включает в себя все необходимые программно конфигурируемые подсистемы – программно определяемые, комплектующие под задачу вычислительное поле мощных серверов и систему хранения данных, коммуникационные сети, подсистемы электропитания, охлаждения и пожаротушения. Все эти подсистемы полностью интегрированы и управляются с помощью вертикально интегрированного программного стека «РСК БазИС».



www.rscgroup.ru

Дизельные генераторы для ЦОДов

ГК ТСС представила дизельную электростанцию TBd 2150 TS с мощностью 1540 кВт (data center prime). Установка предназначена для основного или резервного электроснабжения в наиболее ответственных областях, где требуются высокая надежность источника электроэнергии, высокая мощность и недопустимы перебои в энергоснабжении. Одна из сфер применения – резервное электроснабжение ЦОДов.

Установка TBd 2150 TS выполнена на базе двигателя Moteurs Baudouin 16M33G2000/5 и генератора Evotec. Кроме того, в комплектацию входят рама с антивибрационными опорами, промышленные глушители, система управления.

Основные характеристики электростанции:

- мощность DCP – 1540 кВт (1925 кВА);
- класс качества электроснабжения – G3;
- экологический класс – Stage II;
- расход топлива при 100%-ной нагрузке – 401 л/ч;
- ресурс работы до капитального ремонта – 32 тыс. моточасов.

Электростанция может поставляться в комплектации как для основного, так и резервного применения, с автоматическим запуском и переключением нагрузки при отказе внешней сети и остановкой в случае ее восстановления. В исполнении для резервного использования электростанция штатно оснащается электроподогревателем охлаждающей жидкости и автоматическим зарядным устройством аккумулятора. Объем системы охлаждения – 400 л.

В зависимости от мощности ЦОДа электростанция может комплектоваться генераторами различных марок и мощностей, а также различными моделями двигателей Moteurs Baudouin.

www.tss.ru



СВОБОДНЫЕ ТЕХНОЛОГИИ ИНЖИНИРИНГ

Тел.: (495) 120-2866
E-mail: info@sv-tech.ru
www.sv-tech.ru с. 23

EMILINK GROUP

Тел.: (800) 777-1300
E-mail: info@emilink.ru
www.emilink.ru с. 56-57

IXCELLERATE РОССИЯ

Тел.: (495) 800-0911
E-mail: info@ixcellerate.ru
www.ixcellerate.ru 1-я обл.

KEY POINT

Тел.: (800) 600-3557
E-mail: info@dc-keypoint.ru
www.dc-keypoint.ru 4-я обл.

PATCHWORK

Тел.: +375 17 259-0534
E-mail: info@patchwork.by
www.patchwork.by с. 50-51

SYSTEME ELECTRIC

Тел.: (495) 777-9990
E-mail: ru.ccc@se.com
www.systeme.ru с. 42-43

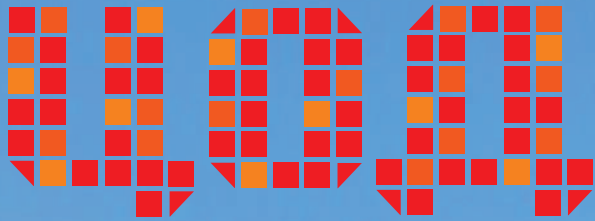
Указатель фирм и организаций

«1С» 21	IEC 44, 46	Turbonomic 65	Корпорация развития
3data 5, 13	iKS-Consulting 4, 5, 7, 10,	UIPath 22	Дальнего Востока и Арктики . 13
#CloudMTS 60 11, 12, 13, 54, 59	Uptime Institute 8, 11, 13, 28,	«Лаборатория
ABBY 22	GK Innostage 75 29, 31, 35, 38, 40, 41	Касперского». 71, 75
Alias Group 5	Intelvision 73	Uptime Institute Intelligence 35,	ГК ЛАНИТ 47
Alibaba Cloud 63	IoT Analytics 73 36, 37, 38, 39, 40, 62, 65	«ЛАНИТ-
Amazon Web Services 63, 65	ISO 44, 46	Vertiv 30	Интеграция» 47
ANSI 13, 44	Ivanti 21	VMware 12, 61, 65	«Магнит» 20
Anti-Malware 75, 76	IXcellerate 5, 13, 28, 30, 31	Wi-Fi Alliance 47, 49	МВД 78
ASHRAE 29, 38	Jet Infosystems Central Asia. 9	X5 Retail Group 20	«МегаФон» 13, 59
Asus 48	Key Point. 9, 12, 13	xFusion. 9	МИД России 52
Automation Anywhere 22	Kofax 22	Zendesk 21	Минцифры России 6, 13,
Baudouin Moteurs 79	Konica Minolta 20	«Авантаж». 60 55, 73, 78
Bi.zone 77	KVM 12	«Аладдин Р.Д.» 54	Минэкономразвития 4
Blue Prism 22	Linode 64	«АльтЭль» 53	МТС 13, 60, 71, 72, 73
C3 Solutions 9	Linux Foundation 67	«Амикон» 53	МТУСИ. 44
Check Point 61	LoRa Alliance 73	АНО «Координационный	«Мультифактор» 54
CipherCloud 61	Microsoft. 12, 21, 52,	совет по ЦОДам и облачным	«НТЦ Атлас». 53
Cisco 52 61, 63, 65, 67	технологиям». 6	НТЦ «Механотроника» 5
Citrix 52	Motorola 48	АНО «Умный многоквартирный	«Оранж Бизнес Сервисез». 78
CommScope 51	Naumen 21	дом» 73	«ПламСпейс». 14
Corning 51	Nutanix. 61	«Базис» 60	ПСБ 18
Cowbell 76	OpenText. 20	Банк России 17, 18, 19, 77, 78	Роскомнадзор 78
DCConsult 32	Oracle 61	ВТБ. 18	«Ростелеком». 13, 54
Deloitte 71	Orange Business Services 54, 78	«Вымпелком». 5, 13	ГК РСК. 79
Delta Electronics 8	OVHcloud 35, 64	«Газпром». 31	«РТК-ЦОД» 6
DigitalOcean. 64	Oxygen. 4, 61	Главный радиочастотный	«Русагро» 60
Docsvision 21	Panduit. 51	центр. 78	Сбербанк 13
DSS. 8	Patchwork 50, 51	«Группа ГАЗ» 52	«Свободные Технологии
Emilink 9, 56	Positive Technologies. 75	«ДатаДом» 24	Инжиниринг» 5, 9
Evotec 79	QazCloud 10, 11	«Диджитал энерджи» 60	«Скала софтвр». 60
Forcepoint 61	RCNTEC 54	«Ди Си квадрат» 9, 12	«Сколково» 14
Fortune Business Insights 71	Sabey 70	ДКС 6	«С-Терра СиЭсПи». 53
Gartner. 20	Samsung. 30	ЕАЭС. 50	«Тионикс» 60
Google 12, 67	SAP. 20, 21, 61	«ИКС-Медиа». 4, 7, 10, 59	«Транстелеком» 10, 11, 12
Google Cloud 63, 65	Schneider Electric 5, 8, 9, 12,	«ИнфоКрипт» 53	ГК ТСС. 53, 79
GreenBushDC. 60 42, 43, 71	«Информзащита» 76	«Фактор-ТС» 53
Group-IB. 77	ServiceNow 65	«Инфосистемы Джет». 59, 60	Федеральное казначейство. 18
GSMA 73	Siemens 16	«ИнфоТеКС» 53, 54	Федеральная
H3C. 9	Siemon. 9	«ИТ Град» 11	таможенная служба 13
Huawei 7, 8, 52	Sigfox 73	«Казахтелеком» 10, 11	ФСК 31
Huber+Suhner 51	Symantec 61	«Казтелепорт» 10, 11, 12	«Элвис-Плюс» 53
IBM. 16, 22, 65, 71	Systeme Electric 5, 9, 42, 43	«Кей Поинт Групп» 5	«ЭлектроМоноблок». 5
IBM Cloud 63	TIA 13, 44	«Код Безопасности». 53	«Яндекс» 11, 13

Учредитель журнала «ИнформКурьер-Связь»:

ООО «ИКС-МЕДИА»:

105082, г. Москва, 2-й Ирининский пер, д. 3.;
Тел.: (495) 150-6424; E-mail: iks@iksmmedia.ru.



МОДЕЛИ СЕРВИСЫ ИНФРАСТРУКТУРА

4-я ежегодная конференция и выставка

Екатеринбург 24 ноября 2022
Hyatt Regency Ekaterinburg

На конференции традиционно рассматриваются вопросы развития индустрии дата-центров и облачных сервисов на территории УрФО и восточных регионов страны, а также основные аспекты создания, эксплуатации и управления ЦОДами.

- Дата-центры на Урале, в Сибири и на Дальнем Востоке
- Карта вендоров для ЦОДов: представленность и потенциал
- Инженерная инфраструктура для дата-центров
- Модульные и контейнерные ЦОДы
- Услуги коммерческих ЦОДов и облачные сервисы



подробно о программе и участниках
на сайте конференции ekb.dcforum.ru



16+

Реклама

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

ОРГАНИЗАТОРЫ



ПРИ
ПОДДЕРЖКЕ
И УЧАСТИИ



Минцифры
РОССИИ



КООРДИНАЦИОННЫЙ СОВЕТ
ПО ЦОДАМ И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ
Автономная некоммерческая организация

UptimeInstitute®

ДАТА-ЦЕНТР KEY POINT



ПЕРВЫЙ. ЕДИНСТВЕННЫЙ.

НА ТЕРРИТОРИИ ДАЛЬНЕГО ВОСТОКА И ВОСТОЧНОЙ СИБИРИ



франшиза

TIER III
сертификат
Uptime Institute

10 МВт
общей
мощности

880
серверных
стоек

ввод в эксплуатацию
первой очереди –
декабрь 2022

Реклама

ДВФО, Приморский край,
ТОР «Надеждинская»



+7 800 600 3557
info@dc-keypoint.ru
dc-keypoint.ru