

ТЕМА НОМЕРА

РОССИЙСКОЕ ПО ДЛ ОБЛАКОВ: ВЫБОР ЕСТЬ

Космос as a Service	36	Жизнь после VMware	63
Как выбрать ИБП для ЦОДа	41	Российские решения SD-WAN	73

ИнформКурьер-Связь

ИКС

издается с 1992 года



Александр Мартынюк

Основатель и исполнительный директор «Ди Си Квадрат»

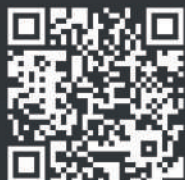
Профессионализм в квадрате



Новинка для центров обработки данных — монтажные шкафы Systeme Electric, серии Uniprom Rack.

Максимум удобства, надёжности, совместимости
и безопасности в одной конструкции.

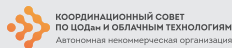
- Поставляются в собранном виде и готовы к установке сразу после распаковки;
- Усиленный каркас из двух сварных рам и продольных швеллеров с новой системой крепления монтажных направляющих;
- Высокая нагрузочная способность: статическая — 1800 кг, динамическая — 1050 кг;
- Перфорированные двери с повышенной вентилируемой площадью;
- Увеличенные кабельные вводы;
- Встроенные крепёжная арматура для соединения нескольких шкафов в ряд.



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», 2023

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: 03.03.23.
Дата выхода в свет: 14.03.23.
Тираж 5 000 экз. Свободная цена.
Формат 64x84/8
Типография: ООО «ПРОПЕЧАТЬ»,
адрес типографии 119618, г. Москва,
Боровское ш., дом 2А, корп. 4, кв. 260.

ISSN 0869-7973

От СКС до облаков



Этот номер журнала выходит в преддверии двух весенних конференций, организуемых «ИКС-Медиа»: 21 марта состоится Cloud & Connectivity, а 11 апреля – «СКС-2023: ЦОДы, офисы, общественные пространства».

Форум Cloud & Connectivity проводится с 2015 г., но ранее был известен как Cloud & Digital Transformation. Почему от модного словосочетания «цифровая трансформация» мы отказались в пользу «связности»? Решили сосредоточиться на актуальных вопросах, прямо касающихся облачных технологий и услуг, которые в непростых условиях пандемии и жестких санкций остаются стабильно растущим сегментом ИТ-рынка. Это обусловлено как экономическими преимуществами облачной модели, особенно в условиях нестабильности и неопределенности, так и повышением доверия к облакам со стороны бизнеса и государственных заказчиков.

Хорошая связность становится неотъемлемой частью облачного ландшафта. Это основа эффективности и надежности облачной среды. Сегодня все больше компаний используют несколько облаков (мультиклауд), а также сочетают облака и собственный ЦОД (гибридная модель). Соответственно все большее значение приобретает надежная и высокоскоростная связность между разными облаками, коммерческими и корпоративными ЦОДами. Традиционные телеком-операторы интенсивно развивают облачный бизнес, а коммерческие ЦОДы все активнее занимаются пирингом. Короче говоря, облака, лежащие в их основе ЦОДы и обеспечивающие связность ИТ-комплексов телекоммуникационные системы – триада бизнеса операторов и провайдеров.

Форум «СКС-2023» – первое и единственное на рынке мероприятие, посвященное тематике структурированных кабельных систем. К его проведению нас подтолкнули главным образом заказчики из отрасли ЦОДов. Основные игроки рынка СКС – западные компании (CommScope, Panduit, Corning...) – прекратили работу в России. «Поляна» опустела. Поэтому важно познакомиться с новыми, в основном российскими, игроками, посмотреть, насколько конкурентны их продукты в непростом сегменте высокопроизводительных и высокоплотных цодовских систем. Не менее интересен и сегмент офисных комплексов. Без качественной СКС такие комплексы не смогут перейти на модель «офис как сервис» с полным обеспечением клиентов необходимым набором ИКТ-сервисов, а это вопрос выживания для их владельцев.

Несмотря на известные трудности, цифровая инфраструктура – от СКС до облаков – развивается, и это абсолютно необходимое условие эффективного функционирования экономики и страны в целом.

До встречи на Cloud & Connectivity и СКС-2023,
Александр Барсков

Российские облака и платформы виртуализации: смена вендоров

с. 20

1 КОЛОНКА РЕДАКТОРА

4 ИКС-Панорама

- 4 Первые итоги года подвели в Екатеринбурге
- 8 ДАЙДЖЕСТ ОТРАСЛИ ЦОДов

10 Экономика и бизнес

- 10 Э. Лоуренс, Р. Асьерто, Д. Бизо, О. Роджерс, Ж. Дэвис, М. Смолак, Л. Саймон, Д. Доннеллан. Пять прогнозов для ЦОДов на 2023 год
- 16 А. Мартынюк. «Нам нужно, чтобы у заказчика было лучшее решение»
- 18 Key Point – крупнейший на Дальнем Востоке ЦОД международного уровня

20 Инфраструктура

- 20 Н. Носов. Российские облака и платформы виртуализации: смена вендоров
- 24 Н. Носов. Российские платформы виртуализации: выбор есть
- 27 Н. Носов. Российские облачные платформы: гамбургский счет



Первые итоги года подвели в Екатеринбурге



Пять прогнозов для ЦОДов на 2023 год



А. Семенов. Направления совершенствования групповых оптических разъемов



**Н. Носов.
Домен здоровья**

**Н. Носов.
Время постправды**

с. 66



- 32** С. Рубцов. Новая страница истории GreenBushDC
- 34** Б. Грановский. СКС для ЦОДов
- 36** Н. Носов. Космос as a Service
- 41** И. Денисов. Критерии выбора ИБП для центров обработки данных
- 48** Новинки от EMILINK: кабеленесущие системы NTSS
- 50** А. Семенов. Направления совершенствования групповых оптических разъемов
- 54** А. Брюзгин. «Гиперлайн» выходит в премиум-сегмент

56 Сервисы и приложения

- 56** Н. Носов. Домен здоровья
- 60** А. Головки, А. Залманова, К. Осташов. Российские почтовые и коммуникационные платформы: какую выбрать
- 63** В. Попов. Жизнь после VMware

66 Безопасность

- 66** Н. Носов. Время постправды
- 70** И. Шаламов. Технологии обмана на службе безопасности
- 73** Н. Носов. Российские SD-WAN и безопасность корпоративных сетей

76 Новые продукты

- 78** Перечень публикаций журнала «ИКС» за 2022 год

Первые итоги года подвели в Екатеринбурге



Несмотря на трудности, российский рынок ЦОДов сохраняет позитивную динамику. Ситуация с доступностью технологий вполне рабочая, а вот с кадрами – серьезные проблемы.

Прошедшая в Екатеринбурге 4-я ежегодная конференция «ЦОД: модели, сервисы, инфраструктура» стала площадкой для подведения предварительных итогов столь непростого 2022-го. Мероприятие, традиционно организуемое «ИКС-Медиа», собрало более 350 делегатов.

На позитивной волне

Российский рынок коммерческих ЦОДов продолжает расти: по предварительным данным iKS-Consulting, к концу 2022 г. количество стойко-мест в них должно увеличиться до 55,7 тыс. единиц. Темп роста – 6% – ниже, чем в 2021 г. (8,4%), но развитие идет по базовому сценарию, и у аналитиков пока нет оснований менять прогноз на негативный.

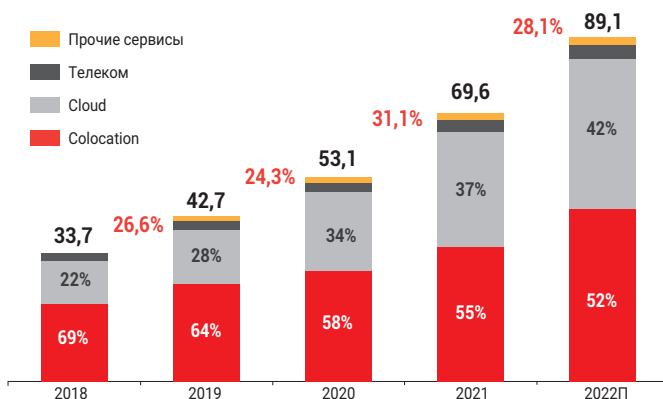
Если же оценивать рынок по объему подведенной электрической мощности (это, возможно, более точный индикатор), то в 2022 г. рост составит около 20%

(в 2021-м – 24%), а суммарная мощность – 668 МВт. В пересчете на стойку средняя подведенная мощность достигнет 8,6 кВт (в 2021 г. – 8,1 кВт).

Общая выручка на рынке коммерческих ЦОДов в 2022 г. должна увеличиться примерно на 28% до 89,1 млрд руб (см. рисунок). «Рынок прошел отметку \$1 млрд. Да, рост несколько замедлился, но по сравнению с другими отраслями экономики он потрясающий. Поэтому деньги для новых проектов доступны. Более того, ЦОДы становятся аккумуляторами инвестиций, которые будут перетекать и из других секторов», – считает Дмитрий Горкавенко, директор по развитию бизнеса iKS-Consulting.

В структуре выручки коммерческих ЦОДов все большую долю занимают облачные сервисы – за год она выросла с 37 до 42%. Именно эти услуги являются основой общего роста отрасли. Рынок инфраструктурных облачных сервисов (IaaS и PaaS) в 2022 г., по предварительным оценкам, увеличится почти на 42% – очень позитивная динамика.

Структура выручки (млрд руб.) на рынке коммерческих дата-центров в РФ, 2018-2022 г.



А. Мартынюк

Ложка дегтя... и надежда на регионы

При вполне достойных темпах роста российского рынка ЦОДов его позиции в мире, увы, ухудшаются. Пять лет назад, когда стартовала амбициозная программа «Цифровая экономика», Россия на мировом рынке услуг colocation занимала 0,7% и упомянутая программа предполагала увеличение этого показателя до 5%. Сегодня

же он снизился до 0,4%. На такую отрицательную динамику обратил внимание Александр Мартынюк, сооснователь проекта Key Point и исполнительный директор компании «Ди Си Квадрат».

Для того чтобы изменить эту динамику, надо резко повысить темпы роста российского рынка, который традиционно концентрируется в Москве и Санкт-Петербурге. Один из путей – развитие дата-центров в регионах. Именно на построение региональной сети ЦОДов нацелен проект Key Point, которые предполагает создание в течение пяти лет 35 объектов общей мощностью 123 МВт и емкостью 10,3 тыс. стойко-мест.

В качестве предпосылок развития региональных ЦОДов А. Мартынюк называет высокий спрос на услуги дата-центров в промышленно развитых регионах, необходимость локального размещения ресурсов компаний, тенденцию отказа заказчиков от капитальных затрат в пользу сервисной модели, а также вступивший в силу с января 2022 г. запрет для ФОВИВ строить собственные ЦОДы.

В рамках проекта Key Point уже введен в эксплуатацию первый объект на 440 стоек во Владивостоке. В 2023–2024 гг. планируется в этом ЦОДе построить вторую очередь еще на 440 стоек, а также – объекты в Новосибирске (800 стоек), Южно-Сахалинске (60 стоек) и Екатеринбурге.

ЦОД в Екатеринбурге будет создаваться в тесном сотрудничестве с «ВымпелКомом». Соглашение об этом подписали 24 ноября 2022 г. «Билайн бизнес» (структурное подразделение «ВымпелКома») и компания Key Point Group. Согласно договоренностям, «ВымпелКом» передает в собственность Key Point Group участок в Екатеринбурге вместе со зданием площадью 3200 кв. м. Здесь к концу 2023 г. будет создан коммерческий дата-центр региональной сети Key Point, ключевым клиентом которой станет «ВымпелКом». Новый ЦОД с отказоустойчивостью уровня Tier III рассчитан на 300 ИТ-стоек со средней мощностью 7 кВт. Общая мощность объекта составит 4 МВт.

ЦОД как ИТ-компания

Активно развивает свои ЦОДы еще один участник форума в Екатеринбурге – компания Охуген. За прошедший год, как сообщил ее директор по ИТ Александр Будкин, она ввела в строй 750 стойко-мест, доведя емкость своего ЦОДа в московском «Технополисе» до 1500 стоек. Вторая площадка – также в Москве – будет запущена в эксплуатацию в 2023 г. Помимо серверных залов на 2000 стоек, на этом объекте большая площадь выделена под офисы, чтобы стимулировать создание экосистемы.

Охуген делает ставку на развитие дополнительных сервисов, позволяющих комплексно решать задачи клиентов. Компания ориентируется на принцип «все по подписке из облака», и для предоставления облачных услуг

разработала собственную платформу виртуализации на базе KVM. Как отметил А. Будкин, многие заказчики в условиях нестабильности не хотят заключать годовые контракты. Им предлагают готовые отраслевые пакеты облачного ПО, скажем, на месяц, и они могут попробовать и решить, использовать их дальше или нет.

В 2022 г. Охуген сформировала два новых направления. Первое – разработка ПО, в рамках которого компания наращивает собственную экспертизу DevOps и NetOps и готова принимать управление командами ИТ-разработки на себя. Второе – базы данных и СУБД. В этой области наиболее актуальна миграция нагрузки на отечественные платформы. Развивается и направление информационной безопасности. Из-за изменения ландшафта угроз Охуген стала рассматривать ИБ как одну из инженерных систем своего ЦОДа, а с учетом нехватки квалифицированных ИБ-специалистов и потребности в готовых решениях по подписке интегрировала ИБ-инструменты в облачную инфраструктуру.

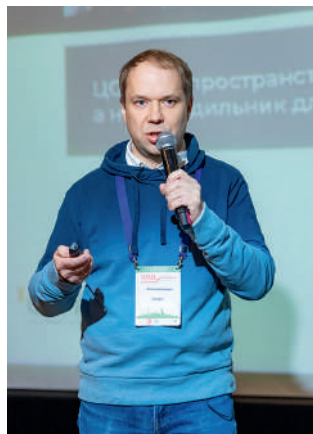
«Облако без системы безопасности – это уже “не комильфо”», – считает Григорий Айкашев, руководитель по внедрению цифровых решений «МегаФона». Наряду с большим портфелем облачных сервисов оператор связи предлагает и базовые услуги colocation. По словам Г. Айкашева, «МегаФон» имеет по всей стране более 120 ЦОДов, которые объединены в единую сеть выделенными каналами с пропускной способностью до 100 Гбит/с на базе магистральной сетевой инфраструктуры компании. За последний год «МегаФон» в семь раз увеличил емкость свободных ресурсов облачной инфраструктуры.

Новые реалии

Лидер российского рынка коммерческих ЦОДов и владелец крупнейшей сети региональных дата-центров компания «Ростелеком-ЦОД» поделилась опытом реализации своего проекта в Екатеринбурге. Первая очередь ЦОДа «Екатеринбург» на 216 стоек была построена за рекордные 11 месяцев и введена в строй в ноябре 2019 г. Поскольку емкости этой очереди были быстро раскуплены, компания почти сразу приступила к реализации второй очереди – еще на 216 стоек. Завершить ее строительство намечено в 2023 г. В планах еще две очереди на той же площадке: третья – на 800 стойко-мест и четвертая – на 216 стойко-мест.

Вторая очередь ЦОДа в Екатеринбурге строится не так быстро, как первая. Одна из причин – смена ряда технологий инженерной инфраструктуры, обусловленная покупкой компании DataLine. Так, если в первом ЦОДе применялась чиллерная система охлаждения, то для второго была выбрана фреоновая, для которой требуются более короткие трассы, что потребовало изменения проекта.

В числе трудностей, возникших после февраля 2022 г., Денис Тарасов, директор дата-центра «Екатеринбург», назвал закрытие официальных каналов поставки и поддержки оборудования европейских брендов, снижение квалификации строительных рабочих из-за сокращения реальных доходов и подорожание стройматериалов.



А. Будкин



На панельной дискуссии. Слева направо: Т. Толмачева (iKS-Consulting), П. Кулаков (Oxugen), Е. Вирцер («Свободные Технологии Инжиниринг»), Д. Тарасов («РТК-ЦОД»), О. Сидоров (УЦСБ)

В частности, из-за резкого повышения цены на медь во второй очереди перешли на алюминиевые кабельные линии 0,4 кВ, что позволило сэкономить 1 млн руб.

В треугольнике «сроки – цена – качество» компания, по словам Д. Тарасова, выбрала путь сохранения цены и качества в ущерб срокам. Был изменен подход к приемке оборудования: если раньше с учетом опыта построения ЦОДа на оборудовании известных брендов нагрузочное



Д. Тарасов

тестирование проводилось только на этапе комплексных испытаний, а индивидуальные испытания выполнялись без полной нагрузки, то сейчас нагрузочное тестирование на номинал проводится для каждой подсистемы. «Выбор новых поставщиков с более низкими ценами позволил остаться в рамках бюджета проекта, несмотря на подорожание стройматериалов и повышение материалоемкости», – отметил Д. Тарасов.

«У нас есть кондиционеры, которые куплены при курсе 60 руб. за евро, и есть – при курсе 120 руб. за евро, и мы их очень бережем, – с улыбкой рассказал Евгений Вирцер, сооснователь проекта Key Point и генеральный директор компании «Свободные Технологии Инжиниринг». – Но все равно по Владивостоку (ЦОДу Key Point во Владивостоке. – Прим. ред.) вписываемся в запланированный рублевый бюджет».

«Для нас основная проблема в том, что сильно снизилась ответственность контрагентов. Поставщики, подрядчики стали гораздо хуже исполнять свои обязательства. У всех появились отговорки... Сегодня никому нельзя верить. Это самый большой риск», – с сожалением констатировал Е. Вирцер.

Кадры как главная проблема

Проблема кадров для отрасли ЦОДов всегда стояла остро. События последнего года никак не способствовали

улучшению ситуации. «Проблема – общая психологическая атмосфера в коллективе. Настроение у сотрудников не самое лучшее. На первое место выходит мотивация, надо вдохновлять людей на работу», – признал Д. Тарасов.

«Уезжают инфраструктурщики, обслуживание оборудования приходится передавать на аутсорсинг. Основные усилия сегодня направлены на то, чтобы люди верили в завтрашний день», – рассказал Павел Кулаков, генеральный директор Oxugen.

«Резкий переход на новые марки оборудования потребовал оперативного переучивания сотрудников. Ушли вендоры с сервисными службами: если раньше можно было рассчитывать на них, то теперь все приходится делать своими силами. В новых проектах оборудование устанавливается, а запускать его бывает некому», – поделился проблемами Олег Сидоров, руководитель направления инженерной инфраструктуры ЦОД компании УЦСБ.

Изменения в кадровой политике отметил и Д. Горкавенко: работодатели стали лояльнее относиться к кандидатам старшего возраста и женщинам. Сотрудники, в свою очередь, также снижают требования к работодателям.

Оборудование: больше российского

Характеризуя ситуацию, сложившуюся на рынке решений для дата-центров после февраля 2022 г., Кирилл Сольев, руководитель отдела инженерной инфраструктуры ЦОД компании Softline, отметил, что если раньше у компаний было четкое понимание рынка и одобренный руководством вендор-лист, то теперь нет ни понимания рынка, ни доверия к новым поставщикам. В текущей ситуации он рекомендует заказчикам заранее формировать вендор-лист, учитывая гарантийные условия и уровень поддержки производителя в том регионе, где реализуется проект, а сроки проектирования и выполнения проекта устанавливать с запасом.

В новых вендор-листах все больше места занимают российские производители, которые продолжают расширять свои предложения. Так, компания Emilink анонсировала на конференции включение в свой портфель выпускаемых по OEM-схеме ИБП и кондиционеров. С учетом широкой номенклатуры изделий, производимых на собственных предприятиях: шкафы/стойки, си-

стемы изоляции коридоров, PDU, СКС, – Emilink теперь способна предложить полное комплексное решение, охватывающее все основные инженерные системы.

Компания С3 Solutions также завершает формирование полного решения для инженерной инфраструктуры ЦОДов, в которое уже входят шкафы, PDU, ИБП и кондиционеры. В Екатеринбурге она представила систему управления инфраструктурой ЦОДов под амбициозным названием «Космос», а также анонсировала разработку собственной СКС, которая скоро появится в продаже.

В условиях нестабильности на рынке крайне важна открытость решений и отсутствие жесткой привязки к конкретному вендору. Это касается и систем управления. О. Сидоров привел пример, когда при смене оборудования охлаждения заказчик был вынужден полностью заменить и систему управления, поскольку прежняя система была жестко привязана к конкретному оборудованию и оказалась несовместима с новым. УЦСБ представила на конференции свою разработку – автоматизированную систему мониторинга и управления Datcheck. Ее отличительные черты – открытость и универсальность, она устанавливается практически на любую программную платформу, включая отечественные среды виртуализации и операционные системы, а также использует отечественные контроллеры и датчики.

В региональных проектах, особенно реализуемых в труднодоступных местах, целесообразно применять модульные ЦОДы высокой заводской готовности. Речь идет о решениях, в которые уже установлено все необходимое инженерное оборудование, а потому при развертывании на месте не нужны высококвалифицированные специалисты. Именно такие решения представила на форуме екатеринбургская компания «Датарк». Перечисляя преимущества модульных ЦОДов высокой заводской готовности, Евгений Тропин, технический директор «Датарк», назвал минимальные требования к подготовке площадки и быстрый ввод в эксплуатацию. При выборе же компонентов для ЦОДов он рекомендовал ориентироваться на поставщиков, которые имеют производство в России или официальный канал поставки, а также сервисную сеть и склад компонентов.

Следует отметить и единственного зарубежного вендора, представившего свои решения в Екатеринбурге. Это китайская Kehua Tech. Компания показала модульную систему ИБП, которая формируется из компактных модулей мощностью 30 кВт (высотой 2U), 50 кВт (3U) и 100 кВт (3U). При использовании 100-кВт модулей общая мощность одного шкафа может достигать 1,6 МВт. Компания продемонстрировала и интеллектуальную систему литий-ионных аккумуляторов Kehua S3. Это также модульная конструкция с «горячей» заменой. Она снабжена функцией интеллектуального выравнивания токов, которая позволяет совместно использовать старые и новые АКБ и литиевые аккумуляторы разных производителей.

В нынешних условиях сервис, как считает Алексей Лобов, руководитель направления ИБП компании «Парус электро», становится важнее «железа». Оборудова-



ние почти всегда можно привезти – это вопрос времени и денег, а вот если вендор отказал в сервисном обслуживании, то у заказчика могут возникнуть серьезные проблемы. Компания «Парус электро» предлагает для рынка ЦОДов модульные ИБП СИП380А МД. Решение строится из силовых модулей на 20 и 50 кВт, устанавливаемых в универсальные кабинеты. И, конечно, она обеспечивает свое оборудование всем необходимым сервисом, включая гарантийное и постгарантийное обслуживание, аудит энергосистемы, предпроектные и проектные работы и пр.

Были представлены в Екатеринбурге и инновационные решения. Так, санкт-петербургская компания Antarctic рассказала о своей системе охлаждения ERA на основе фрикулинга с адиабатическим доохлаждением. Ее изюминка – теплообменник на основе графена, на который можно подавать воду любого качества, даже морскую. При этом трубки не окисляются, не корродируют и не закупориваются, на них не осаждаются соли и минералы. По словам Виктора Гагуа, генерального директора Antarctic, систему ERA уже планируется задействовать в четырех цодовских проектах.

Хотя в ЦОДах традиционно устанавливают дизель-генераторы, возможные варианты систем автономной генерации ими не ограничиваются. Дмитрий Иванов, директор департамента развития и маркетинга ТХ «Электросистемы», предлагает использовать для этой цели энергетические комплексы на основе газопоршневых двигателей, которые активно применяются на различных объектах. Дополнение таких комплексов абсорбционными холодильными машинами позволит одновременно получить и столь необходимый ЦОДам холод. По расчетам, которые привел Д. Иванов, благодаря этому решению можно до 30% сократить срок окупаемости проекта ЦОДа.

Время перемен, переживаемое сейчас отраслью, дает хороший шанс не только новым производителям, но и новым техническим решениям. Главное – избежать технологической деградации, обеспечив высокий уровень надежности объектов.

Александр Барсков
Екатеринбург – Москва



НОВОСТИ АНО КС ЦОД

ЯНВАРЬ 2023

Сотрудничество между АНО КС ЦОД и Министерством цифрового развития Казахстана

АНО «Координационный совет по ЦОДам и облачным технологиям» и Комитет телекоммуникаций Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан подписали меморандум о взаимопонимании. В документе определены основные направления сотрудничества в области развития информационной инфраструктуры, ЦОДов, облачных технологий и точек обмена интернет-трафиком (пиринговых центров). Партнеры намерены, в частности, содействовать инициированию и продвижению проектов построения ЦОДов и внедрению облачных технологий; распространению лучших практик поддержки предпринимательства в целевых областях, а также разработке системы прогнозирования потребностей в услугах хранения и обработки данных бизнеса, государства и граждан на территории Республики Казахстан.

О текущих задачах и планах АНО КС ЦОД на 2023 г.

31 января состоялась встреча участников АНО КС ЦОД, в состав которой входят лидеры рынка ЦОДов, облачного провайдинга, крупнейшие поставщики решений. Основной повесткой встречи стало освещение планов деятельности АНО в 2023 г., текущих вопросов, а также обсуждение новых программ, инициированных совместно с Минцифры России. В 2022 г. участниками АНО КС ЦОД была разработана и утверждена «Модель классификации ЦОДов», сейчас продолжается работа над методикой технологического аудита ЦОДов для целей классификации по указанной модели. В фокусе новых совместных инициатив Минцифры и АНО – разработка программ, направленных на популяризацию сервисной модели для развития отечественного рынка облачных услуг и ускорения ввода новых мощностей ЦОДов, прежде всего способствующих расширению региональной ИКТ-инфраструктуры.

НОВОСТИ ОТРАСЛИ

«Карта вендоров ЦОД»

Чтобы помочь заказчикам сориентироваться в новых условиях и принимать более обоснованные решения при выборе оборудования, эксперты iKS-Consulting разработали новый инструмент – «Карту вендоров ЦОД», которая показывает позиции основных производителей по двум измерениям: представленность (оценка присутствия решений вендора в инфраструктуре и восприятии заказчиков) и потенциал (оценка способности вендора к развитию в РФ в текущих условиях). На карте собраны данные по четырем

укрупненным продуктовым сегментам: ИБП; СКС; системы кондиционирования/вентиляции и ИТ-стойки.

ЦОды Key Point



Компания Key Point запустила в промышленную эксплуатацию первый на Дальнем Востоке и в Восточной Сибири коммерческий ЦОД международного уровня. Объект емкостью 880 ИТ-стоек и мощностью 10 МВт, прошедший сертификацию Uptime Institute по уровню надежности Tier III, реализуется по модульной технологии в две очереди. Первая включает строительство двух технологических модулей общей емкостью 440 стоек со средним энергопотреблением 5 кВт.

Также начато проектирование дата-центра Key Point в Екатеринбурге. Объект площадью 3200 кв. м будет построен внутри существующего здания. Он рассчитан на 300 ИТ-стоек средней мощностью 7 кВт. Общая мощность объекта составит 4,0 МВт. Новый ЦОД планируется сертифицировать на соответствие Tier III. Ввод объекта в эксплуатацию запланирован на декабрь 2023 г.

IXcelerate обновила сертификаты ISO

По итогам внешнего аудита компания обновила сертификаты соответствия двум международным стандартам – ISO 9001:2015 «Системы менеджмента качества» и ISO 45001:2018 «Системы менеджмента безопасности труда и охраны здоровья». Аудитором выступила международная группа компаний TÜV Austria,

имеющая один из самых узнаваемых в мире брендов. Ее сертификаты признаются на самом высоком уровне. В этом году IXcelerate намерена также получить сертификат на соответствие стандарту ISO/IEC 27001 в сфере информационной безопасности.

Казахстанский рынок ЦОДов быстро растет



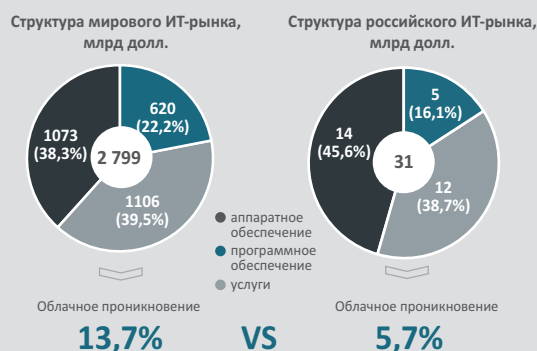
Казахстанский рынок коммерческих ЦОДов развивается стремительно. По данным iKS-Consulting, за последние три года его емкость удвоилась и достигла 2450 стойко-мест (данные на конец 2022 г.). А в предстоящие три года он вырастет еще на 50%, до 3670 стойко-мест. Хотя большинство корпоративных заказчиков пока используют собственные серверные и небольшие ЦОДы, уже многие охотно идут в коммерческие дата-центры. По свидетельству ведущих операторов ЦОДов, таких как «Казахтелеком» и «Казтелепорт», они уже испытывают дефицит свободных мест. Поэтому можно ожидать начала массового строительства новых объектов.

Softline запустила ЦОД в Беларуси

Уровень нового ЦОДа соответствует Tier II+, обеспечен высокий уровень охраны, пожароустойчивости и охлаждения. При этом Softline берет на себя финансовую ответственность в случае отказа мощностей, гарантируя SLA до 99,982% в зависимости от выбранной конфигурации. Дата-центр рассчитан на 38 стойко-мест, основными клиентами станут компании из России и Беларуси.

97% компаний в России не используют инфраструктурные облака

Лишь менее 3% российских компаний использовали облачные технологии в 2022 г. А доля облачного сегмента на ИТ-рынке России в 2,4 раза ниже глобальных показателей. Об этом говорится в совместном исследовании Cloud и «Технологии Доверия». Вместе с тем, согласно данным исследования, за последние три года количество компаний, использующих облачную инфраструктуру, утроилось. Лидерами по затратам на облачные технологии стали финансы (в среднем затраты – 17,8 млн руб. на компанию), ритейл (16,8 млн руб.), ИТ (12,8 млн руб.), развлечения и медиа (7,2 млн руб.).



Источник: Cloud и «Технологии Доверия»; данные за 2021 г.



**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



Пять прогнозов для ЦОДов на 2023 год

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

Эксперты Uptime Institute Intelligence рассматривают некоторые наиболее важные тенденции 2023 г. – от геополитических до технологических, но объединяет их то, что все они затрудняют планирование развития и эксплуатацию ЦОДов.

В начале каждого года эксперты Uptime Institute выделяют основные тенденции – или прогнозы – на ближайший год. Мы стремимся привлечь внимание к жизненно важным, но не самым очевидным вопросам, которые заставляют задуматься. На 2022 г. мы сделали пять прогнозов, которые в значительной степени подтвердились и продолжают оставаться актуальными.

Наши прогнозы на 2023 г. подчеркивают новые или усугубляющиеся проблемы, с которыми сталкиваются операторы ЦОДов. Это не означает, что отрасль находится в кризисе – ЦОДы пользуются высоким спросом и в значительной степени эффективны и устойчивы. Но важно выделить области, где могут потребоваться постоянная бдительность и оперативное реагирование.

Сектор цифровой инфраструктуры последние несколько десятилетий быстро развивался не только из-за кажущегося ненасытным аппетита к цифровым услугам, но и благодаря использованию преимуществ дешевого капитала, глобализации и свободной торговли. Спрос на вычислительные мощности и хранилища остается таким же высоким, как и прежде, однако обстановка на мировом рынке осложнилась.

В 2023 г. и далее многие угрозы развитию и стабильности цифровой инфраструктуры будут заключаться не в проблемах с проектированием или эксплуатацией, а во внешних обстоятельствах. Конфликт на Украине, торговая напряженность между США и Китаем, последствия пандемии COVID-19 привели к высокой инфляции, сбоям в цепочках поставок и нехватке квалифицированных кадров, а быстрый рост цен на энергоносители увеличил затраты на строительство и эксплуатацию ЦОДов.

Операторы ЦОДов реагируют на эти угрозы увеличением своих бюджетов (и более жестким контролем их расходования), продлением сроков эксплуатации оборудования, творческими подходами к устранению задержек в цепочке поставок и к привлечению и удержанию персонала. ЦОДы также готовятся к волне новых нормативных требований в области экологии и энергоэффективности.

Проблем становится больше, но это не означает, что отрасль замедляет свой рост. Большинство владельцев и операторов ЦОДов, недавно опрошенных Uptime Institute, планируют расширить свои площадки. Исследования рыночных и финансовых аналитиков показывают, что спрос на ресурсы ЦОДов остается высоким.

ПРОГНОЗ 1: Проблемы в цепочках поставок сохраняются

Пандемия COVID-19 и последовавший за ней сбой в цепочках поставок продемонстрировали зависимость индустрии ЦОДов от взаимосвя-

занных глобальных рынков и производимых их участниками компонентов. Эти проблемы затронули и многие другие отрасли, но потребность дата-центров в разнообразном и довольно сложном электрическом и механическом оборудовании усугубила их.

Хорошо иллюстрируют ситуацию дизель-генераторы. Они состоят из сотен компонентов, поставляемых по меньшей мере из дюжины стран Северной Америки, Европы и Азии. Нехватка, скажем, регуляторов напряжения, воздушных фильтров, клапанов или клемм аккумуляторных батарей может привести к серьезным задержкам с поставкой ДГУ. Даже когда производство оборудования для ЦОДов (например, свинцово-кислотных АКБ и волоконно-оптических кабелей) относительно локализовано, цены и доступность зависят от меняющейся обстановки на мировых рынках.

Окончание пандемии не означает возвращение к нормальной жизни предыдущих лет, поскольку сохраняются высокий отложенный спрос, более высокие затраты и аномально длительные сроки поставки. Исследование Uptime Institute, проведенное в 2022 г., показывает масштаб проблемы: каждый пятый оператор сообщает о серьезных задержках или перебоях в поставках за предыдущие 18 месяцев. Неудивительно, что почти половина респондентов недовольны по крайней мере некоторыми из своих поставщиков. Наибольшие сложности возникают с основным электрооборудованием (ИБП, ДГУ, распределительными устройствами) и блоками охлаждения. Крупные операторы (несмотря на превосходящую покупательную способность), по-видимому, несут на себе основную тяжесть проблем с поставками.

В общей сложности 40% операторов, принявших участие в опросе, подтвердили, что в ответ на возникшие проблемы они изучают дополнительные источники поставок. Примерно столько же сообщили об увеличении своих запасов запчастей и материалов для соблюдения графиков технического обслуживания и обеспечения эксплуатационной устойчивости. Поставщики приняли аналогичные меры для устранения дефицита и задержек. По состоянию на вторую половину 2022 г. положение, по-видимому, улучшится, но медленно (рис. 1).

Геополитическая обстановка порождает риски

Геополитическая напряженность – в первую очередь между возглавляемым США западным альянсом, Китаем и, в меньшей степени, Россией – порождает дополнительные угрозы. Даже при диверсификации источников поставок и более высоких целевых показателях запасов

Рис. 1. ►
Операторы констатируют медленные улучшения в цепочке поставок продуктов для ЦОДов
 Источник: Uptime Institute

Что из приведенного ниже лучше всего описывает общую ситуацию с поставками продуктов для ваших ЦОДов за последние шесть месяцев?



индустрия ЦОДов остается особенно подверженной рискам, создаваемым текущей геополитической обстановкой.

Профиль этих рисков резко отличается от последствий других крупных событий, сколь бы редкими они ни были. В отличие от пандемии, стихийного бедствия или энергетического кризиса, последствия геополитических событий сложнее смоделировать, поскольку они являются результатом высокоцентрализованного процесса принятия политических решений в Пекине, Брюсселе, Москве и Вашингтоне. Поэтому и разработать эффективные планы действий в чрезвычайных ситуациях сложнее.

Шоковая терапия пандемии COVID-19 сделала отрасли экономики более устойчивыми и внимательными к потенциальным сбоям в будущем. Тем не менее, если некоторые из наиболее радикальных угроз, создаваемых нынешней геополитической ситуацией, станут реальностью, их последствия, вероятно, будут более длительными и драматичными, чем все, что происходило до сих пор.

Эксперты Uptime Institute видят две основные области, в которых сочетание глобальной взаимозависимости и концентрации делает цифровую инфраструктуру уязвимой для потенциальных экономических и военных столкновений в случае дальнейшего ухудшения геополитической обстановки: это цепочки поставок полупроводников и подводные кабельные системы.

Полупроводники – уникальная проблема

Ничто так ярко не иллюстрирует глобальную взаимозависимость и системную хрупкость, как потребность в передовых полупроводниковых технологиях. Это касается не только ИТ-оборудования: контроллеры, процессоры, микросхемы памяти и силовая электроника есть практически в любом изделии. Чипы служат не только для того, чтобы расширить функциональность или улучшить элементы управления – они вседуши. Некоторые недавние задержки в поставках оборудования для ЦОДов (включая распределительные устройства и ИБП) были вызваны именно нехваткой специализированных чипов.

Цепочки поставок для производства полупроводниковых микросхем охватывают тысячи поставщиков в десятках отраслей, включая сверх-

чистые металлы и газы, химические реагенты, высокопроизводительные лазеры и оптику, различное оборудование для обработки пластин, системы фильтрации для чистых помещений и т.д. На каждом этапе лишь небольшое число поставщиков с высокой квалификацией способны соответствовать требуемым стандартам качества и производительности.

Уровень сложности и специализации, необходимый для производства передовых полупроводниковых микросхем, настолько высок, что ни одна отдельная страна – независимо от того, насколько она велика или богата ресурсами, – не является полностью самодостаточной или станет таковой в разумные сроки и при разумных экономических затратах. Это означает, что множество отдельных точек отказа (и потенциальных узких мест) в цепочке поставок ИТ-оборудования для ЦОДов сохранится.

Многие страны понимают остроту проблемы. Правительство США и Европейская комиссия отреагировали принятием законодательства, направленного на поддержку и стимулирование инвестиций в местные производственные мощности (законы US CHIPS and Science Act и European Chips Act соответственно). Китай, хотя все еще отстает примерно на пять-десять лет от своих западных конкурентов, также продолжает инвестировать в свою полупроводниковую промышленность. Тем временем политические баталии по поводу интеллектуальной собственности продолжаются, сохраняются и проблемы поставок материалов, компонентов и доступа к экспертным знаниям.

Последствия этих законодательных инициатив проявятся, вероятно, лишь через десятилетие и в основном будут связаны с переносом мощностей по производству микросхем. Даже при наличии жесткой политической воли (и безграничной финансовой поддержки частных инвестиций) обеспечение самодостаточности в производстве микросхем на всем пути от добычи сырья до финального продукта выглядит невозможным.

Именно по этой причине все более жесткие меры правительства США, направленные на ограничение доступа Китая к передовым полупроводниковым технологиям, оказываются эффективными. Но именно потому, что они эффективны, ситуация становится все более нестабильной для всей отрасли.

Особую озабоченность вызывает Тайвань. Высокая концентрация мирового производства полупроводников и ИТ-оборудования на острове, где находится крупнейший в мире и наиболее продвинутый кластер контрактного производства микросхем, создает существенные уязвимости в цепочке поставок. Любая серьезная конфронтация (экономическая или военная) может привести к глубоким и далеко идущим нарушениям во всей ИТ-индустрии и многих других отраслях экономики.

Риски, связанные с подводными сетями

Уязвимость подводных волоконно-оптических сетей – еще одна проблема, и, как и в случае с полупроводниками, проблема не новая. Однако растущая геополитическая напряженность повышает риски нарушения их работы отдельными государствами.

Подводные волоконно-оптические сети состоят из сотен кабелей, по которым проходит почти весь межконтинентальный трафик, поддерживающий глобальную экономическую деятельность на триллионы долларов. В настоящее время существует более 500 международных и внутренних сетей, которые принадлежат частным компаниям и управляются почти исключительно ими. Протяженность кабелей этих сетей существенно затрудняет их защиту от потенциальных угроз. Некоторые подводные кабели представляют собой ценные цели для определенных субъектов, а повредить или разорвать их можно втайне и без явных следов атаки.

Большинство обрывов подводных кабелей не приводят к массовым отключениям. Как правило, трафик может быть перенаправлен по другим кабелям, хотя и за счет увеличения задержки. Но когда в одном регионе одновременно прерываются несколько линий, негативный эффект может быть более существенным.

В 2006 г. сильное землетрясение в проливе Лусон (между Тайванем и Филиппинами) привело к отключению семи из девяти подводных кабелей. Это вызвало широкомасштабные перебои в работе информационных сетей по всему Азиатско-Тихоокеанскому региону, что, в свою очередь, привело к сбоям в работе предприятий в Гонконге, Японии, Сингапуре, Южной Корее и на Тайване. Для восстановления этих жизненно важных сетевых подключений было задействовано более 40% мирового парка оборудования для ремонта кабелей. Полностью восстановить связность удалось лишь через семь недель.

Кабели уязвимы и для человеческих действий – как случайных, так и преднамеренных. Наиболее распространенной причиной являются суда, якоря и рыболовные снасти которых могут зацепить и повредить кабель. Известны слу-

чай и злонамеренного повреждения кабелей, например, в случае конфликтов между странами.

Защита от таких угроз, а также обнаружение и мониторинг потенциальных угроз или определение лиц, ответственных за совершение атак, затруднены, особенно при повреждении кабелей протяженностью в тысячи миль. Острова, такие, как Тайвань, особенно уязвимы при атаках на подводные кабели.

- Цепочки поставок оборудования для ЦОДов все еще страдают от длительных задержек, хотя ситуация медленно, но улучшается.
- Текущая геополитическая напряженность представляет новые угрозы, полное воздействие которых трудно моделировать и прогнозировать.
- Наиболее высокие риски связаны с передовыми полупроводниковыми микросхемами, жизненно важными для ИТ-систем и инженерного оборудования ЦОДов.
- Подводные кабельные системы особенно уязвимы для повреждений. Успешно скоординированная атака может иметь серьезные последствия для ключевых цифровых сервисов.

ПРОГНОЗ 2: Переход в облако потребует более тщательного анализа

Крупным облачным провайдерам часто пришлось конкурировать друг с другом, и иногда жестко. Однако им лишь изредка случалось конкурировать с традиционными платформами для корпоративных ИТ. Чаще всего ИТ-директора, ответственные за критически важные ИТ-системы, считают переход в публичное облако не слишком рискованным, гибким, перспективным и в конечном счете недорогим мероприятием. Но так ли это на самом деле?

Предстоящие годы ожидаются экономически и политически беспокойными, риск сбоев в инфраструктуре и цепочках поставок повышается. Это подталкивает компании переносить ИТ-системы в публичные облака. Но для поддержания необходимой отказоустойчивости может понадобиться немало сил и средств.

Картина сложная, требуется учитывать много факторов, но есть некоторые признаки того, что популярность публичных облаков снижается. Amazon Web Services (AWS), крупнейший поставщик облачных услуг, сообщил об историческом замедлении роста во второй половине 2022 г. после почти десятилетнего подъема (на 30–40% каждый год). Microsoft также сообщила о вероятном замедлении роста своего облачного сервиса Azure.

Конечно, никто в отрасли не предполагает, что использование публичных облаков достигло своего пика или что они больше не имеют стратегической ценности для крупных предприятий. Их использование по-прежнему увеличивается и по-

прежнему является движущей силой роста индустрии ЦОДов. Публичное облако останется практически автоматическим выбором для большинства новых приложений. Но организации со сложными, критическими и гибридными системами, скорее всего, замедлят или приостановят миграцию из локальной инфраструктуры в облако.

Закончился ли облачный медовый месяц?

Многие предприятия оказались перед необходимостью быстрого переноса приложений в облако без всестороннего анализа затрат, выгод и рисков. ИТ-директора, часто по настоянию или при поддержке финансовых руководителей либо топ-менеджеров, для новых и/или ключевых проектов отдадут предпочтение облакам, а не локальным ИТ-инфраструктурам.

Данные опроса Global Data Center Survey 2022, проведенного Uptime Institute, свидетельствуют о том, что многие организации отказываются от изначальной настороженности и все более уверенно используют облака для своих самых важных критических рабочих нагрузок. Доля респондентов, не размещающих критически важные рабочие нагрузки в публичном облаке, снизилась с 74% в 2019 г. до 63% в 2022 г.

Нашумевшие истории о сбоях в работе облачных сервисов вкупе с растущим интересом к ним регулирующих органов побуждают некоторых клиентов быть более внимательными. Они начинают понимать, что не все приложения спроектированы таким образом, чтобы воспользоваться преимуществами ключевых облачных функций, а реализация правильной архитектуры приложений может обойтись очень дорого. «Подъем и перемещение» приложений, которые не могут масштабироваться или динамически отслеживать изменения пользовательского спроса (предложение ресурсов), вряд ли задействуют все преимущества облака и могут создать новые проблемы.

Одна из проблем заключается в том, что при переносе в облако во многих приложениях не была изменена архитектура для достижения бизнес-целей, в первую очередь отказоустойчивости. Многие облачные заказчики не в полной мере осознают свои обязанности в отношении обеспечения отказоустойчивости и масштабируемости собственных приложений, полагая, что провайдеры заботятся об этом автоматически. Те же недвусмысленно дают понять, что иногда в некоторых зонах доступности будут происходить сбои, и рекомендуют заказчикам распределять рабочие нагрузки по нескольким зонам, повышая вероятность того, что приложения продолжат функционировать, даже если одна зона выйдет из строя.

Исследования Uptime Institute позволяют оценить, насколько корпоративные заказчики чувствительны к нарушению работы одной зоны доступности. Согласно опросу, проведенному в 2022 г., 35% респондентов считают, что потеря зоны доступности приведет к значительным проблемам с производительностью, а 16% респондентов указали, что потеря зоны доступности не повлияет на их облачные приложения.

Чтобы в полной мере воспользоваться преимуществами облака и снизить риск сбоев, заказчикам необходимо перепроектировать архитектуру своих систем для обеспечения отказоустойчивости. Это увеличивает затраты, что нужно учитывать, принимая решение о переносе приложений из локальной среды в облако. Ранее Uptime Institute установил, что разработка архитектуры приложения для двух зон доступности может стоить на 43% дороже, чем разработка недублированного приложения. Распределение по разным облачным регионам, что еще больше повышает отказоустойчивость, может удвоить затраты.

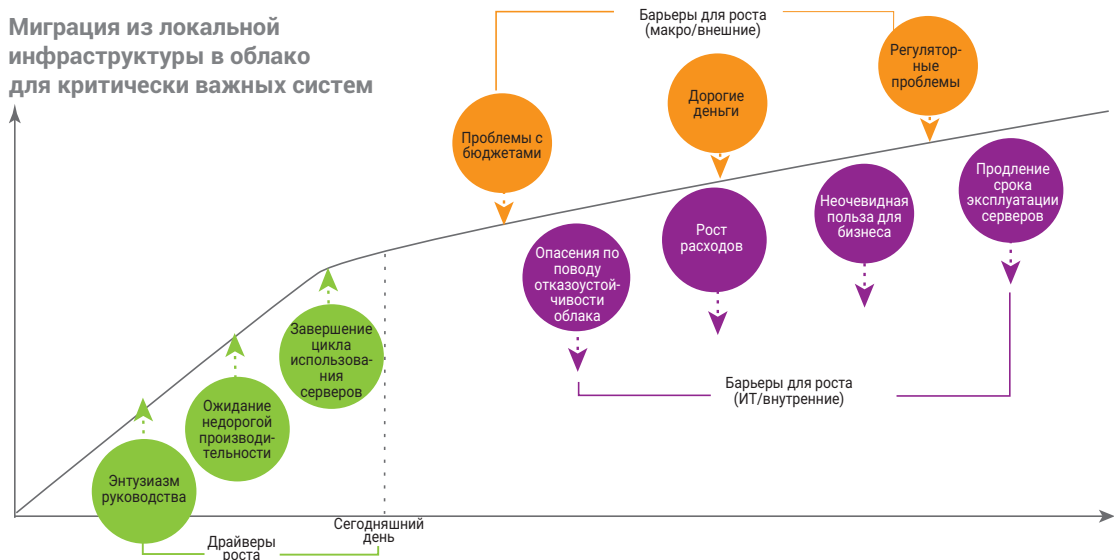


Рис. 2. ▶
Движущие силы и барьеры для миграции в облако (инфраструктурные облачные сервисы)

Источник: Uptime Institute

Экономические факторы снижают привлекательность перехода в облако

Успешная и полнофункциональная миграция критически важных рабочих нагрузок в облако влечет за собой дополнительные затраты, часто существенные. Многие заказчики только сейчас начинают это осознавать.

Затраты возникают как на начальной фазе, когда приложения нужно переработать, чтобы сделать их облачными (а специалисты сегодня в дефиците), так и при эксплуатации, поскольку необходимо поддерживать работу в нескольких зонах. Очевидно, что стоимость облака не всегда учитывалась. Основная причина, по которой организации возвращают свои рабочие нагрузки на локальные площадки из публичного облака, – высокие расходы (на это указали 43% респондентов нашего опроса).

Очередной цикл обновления серверного парка часто служит триггером для миграции в облако. Вместо покупки новых физических серверов ИТ-руководители предпочитают перенести приложения в публичное облако. Глобальный опрос менеджеров ЦОДов, проведенный Uptime в 2015 г., показал, что свои серверы в рабочем состоянии в течение пяти и более лет поддерживали 35% респондентов; к 2022 г. эта доля увеличилась до 52%. В сложной экономической ситуации ИТ-директора могут предпочесть продление срока эксплуатации серверов затратам на миграцию в облако.

Даже если СIO продолжат настаивать на переходе в облако, все равно нужно будет оправдать расходы на миграцию. Несмотря на сокращение затрат на локальную ИТ-инфраструктуру, многие организации не готовы к непредвиденным расходам, требуемым для повышения устойчивости и производительности облачных приложений. Ограниченный доступ к капиталу вкупе с более жестким контролем расходования бюджета заставит руководителей тщательно обдумать необходимость полной миграции в облако.

Дополнительное давление со стороны регуляторов

Правительственные учреждения также начинают беспокоиться о том, что облака недостаточно устойчивы и что они таят другие риски. Доминирование Amazon, Google и Microsoft (так называемых гиперскейлеров) вызвало опасения по поводу риска концентрации – чрезмерной зависимости от ограниченного числа облачных провайдеров – в нескольких странах и ключевых секторах.

Регулирующие органы стараются оценить этот риск и управлять им, опасаясь, что он может угрожать стабильности экономики. Недавно принятый ЕС Закон о цифровой операционной устой-

чивости (DORA, Digital Operational Resilience Act) закладывает основу для того, чтобы возложить ответственность за надзор за поставщиками ИТ-услуг (включая облачные сервисы) на участников финансового рынка. Управление телекоммуникациями правительства Великобритании (Office of Communications, Ofcom) запустило исследование рынка публичных облачных сервисов страны, объем которого составляет 15 млрд ф. ст. Давно действующий, но недавно обновленный закон Грэмма – Лича – Блайли (GLBA, также известный как Закон о модернизации финансовых услуг) в США теперь требует регулярных оценок кибер- и физической безопасности.

Направление ясно. От большего числа организаций потребуется лучше оценивать и планировать риски, связанные со сторонними поставщиками ИТ-услуг. Но сделать это не всегда легко.

Облачные провайдеры сталкиваются с тем же набором рисков (связанных с кибербезопасностью, нехваткой персонала, цепочками поставок, экстремальными погодными условиями, нестабильными электросетями и т.д.), что и другие операторы. Но они редко открыто говорят о проблемах, порождаемых этими рисками.

Законодательство заставит регулируемые отрасли учитывать все риски, прежде чем переходить в публичное облако. Однако большая часть этого законодательства еще в стадии разработки.

Как это повлияет на общий рост публичных облаков и их привлекательность для топ-менеджеров? Гиперскейлеры будут продолжать расширяться по всему миру, создавать новые продукты и услуги. Корпоративные клиенты, в свою очередь, скорее всего, будут и дальше находить облачные сервисы вполне конкурентоспособными. Но перенос рабочих нагрузок замедлится, поскольку заказчики станут более осторожными. Они будут тщательнее оценивать свои риски, разрабатывать архитектуры, помогающие их снизить, и переходить в облако только тогда, когда будут к этому готовы и когда это действительно повысит ценность для бизнеса.

- В период экономической неопределенности стоимость миграции в облако и угроза резкого роста облачных расходов станут сдерживающими факторами для такой миграции.
- Многие ИТ-директора только сейчас осознают проблемы, связанные с обеспечением достаточной отказоустойчивости облака.
- Регулирующие органы и руководители компаний часто только начинают понимать и ограничивать риски, обусловленные высокой зависимостью от публичных облаков.



Окончание статьи – в следующем номере «ИКС»



«Нам нужно, чтобы у заказчика было лучшее решение»

Консалтинг в России – дело непростое, но для индустрии ЦОДов очень нужное. Этому делу посвятил себя Александр Мартынюк. Созданная им компания «Ди Си Квадрат» вот уже 15 лет успешно работает на рынке ЦОДов.



– Александр, почему именно консалтинг, ведь подряды выгоднее?

– Когда я задумался о создании «Ди Си Квадрат», уже посмотрел на рынок с разных сторон: поработал в подрядчике и заказчике, поторговал, занимался монтажом силовых систем, СКС... И у меня сложилось впечатление, что качество продукта, который мы тогда создавали, не соответствовало важности решаемых им задач.

Центры обработки данных – это то, что должно служить долго и максимально надежно. Но существовавшие в то время подходы, культура производства и исполнения не позволяли получить такой продукт. Вот и решил, что консалтинговая компания, которая будет со стороны заказчика формировать постановку задач, требования к качеству и следить за исполнением работ, – это правильно.

К тому моменту я уже много раз побывал в США, посмотрел, как это устроено там. Понял, консалтинг в области ЦОДов – то, чем я хотел бы заниматься. И вот 23 января 2008 г. была создана компания «Ди Си Квадрат».

– 2008-й нельзя назвать простым годом.

– Да, компания была образована прямо перед кризисом. Фирмы закрывались, рынок падал, курсы валют штормило... Но у нас был контракт, который позволял спокойно смотреть на все происходящее и делать свое дело. Мы участвовали в создании штаб-квартиры ВТБ, отвечали за строительство нескольких ЦОДов в башне «Федерация» в Москва-Сити. Первые годы мы не только управляли проектами на стороне заказчика, но и решали практические задачи, связанные с перегревом оборудования, аварийными отключениями электропитания и т.д.

– А когда в России появились ЦОДы, построенные, на ваш взгляд, правильно?

– Первые два полноценных дата-центра – у «Юкоса» и ТНК-ВР – появились в 2004 г. Я руководил проектом ТНК-ВР. Эти ЦОДы проектировались как специализированные помещения со всей необходимой инженерной инфраструктурой, с резервированием, в том числе по внешнему питанию, дизельной поддержкой 2N. Они были рассчитаны на бесперебойную работу в режиме 24/7.

Когда проект в ТНК-ВР завершился, ко мне за консультациями обратились представители Stack Group, они тогда строили М1. Фактически М1 стал первым полноценным коммерческим ЦОДом. Конечно, был объект «Голден Телекома» и другие объекты, на которых размещалось стороннее оборудование, но это были технологические площадки операторов связи, они изначально не проектировались как ЦОДы.

– Что изменилось на рынке ЦОДов за прошедшие 15 лет?

– Проектов стало больше, они значительно крупнее. Тогда мы строили ЦОД на 200 стоек или даже меньше. Сейчас идут проекты на одну, две, три, четыре тысячи стоек. На данный момент у нас в работе почти полтора десятка проектов общей мощностью около 300 МВт.

Скорость принятия решений и скорость строительства увеличились. Раньше на реализацию проекта уходило два года и более. Сейчас все стараются уложиться в год или чуть больше.

Сложность инфраструктуры повысилась. При этом уровень резервирования снизился, по энергетике точно. Раньше все делали 2N, сейчас это дорого. В основном используют дробные схемы резервирования. Это кардинальный шаг, который существенно снижает CAPEX, но предъявляет более высокие требования к проектированию и качеству службы эксплуатации.

Вырос уровень знаний заказчиков о том, что мы делаем. Нельзя сказать, что заказчики уже технически готовы к тому, чтобы самим управлять проектами, но они по крайней мере понимают, что такое ЦОД. И в этом большая заслуга «ИКС-Медиа», вы успешно популяризируете эту тему.

Наконец, сдвинулось с мертвой точки цодостроение в регионах. Начали появляться региональные ЦОДы. Не серверные, не операторские площадки, а именно ЦОДы.

– А в последние два-три года? Пандемия, затем беспрецедентные санкции...

– Число проектов резко подскочило. Это связано, в частности, с выходом на рынок новых игроков. Как правило, у них нет собственной экспертизы, поэтому они обращаются к нам. За два последних года мы увеличили штат компании в два раза. Работы очень много. И сейчас активно набираем сотрудников.

Если говорить о сложностях... Да, многие модели оборудования теперь недоступны, даже отдельные категории решений, например, дизель-динамические ИБП. Но для нас это не стало проблемой. Те же динамические ИБП мы никогда не рекомендовали, считая их не самым надежным решением. Более того, мы никогда не привязывали проектные решения к конкретному оборудованию, опираясь на типовые решения. Выбор по-прежнему есть. Да, он другой. Но важно, что он сохранился.

– А как за 15 лет изменился перечень услуг, которые оказывает «Ди Си Квадрат»?

– Мы его сильно расширили. Раньше были точечный консалтинг и управление проектами. Сегодня делаем техниче-

ский аудит перед сделками M&A, проводим конкурсы по выбору исполнителей, проектировщиков, подрядчиков, производителей оборудования. Это непростой выбор. Все хотят сэкономить, но ЦОДы не те объекты, для которых надо выбирать только по цене. Важно, чтобы все работало должным образом.

Начали заниматься подбором площадок. В этом плане работаем с несколькими агентствами недвижимости. В нашем портфеле услуг – разработка эскизных проектов, финансовых моделей, подготовка бизнес-планов для защиты проектов в целях получения финансирования, надзорное сопровождение строительства.

И последнее, что мы добавили, – commissioning. Это подготовка программ испытаний для приемки инженерной инфраструктуры ЦОДа, подготовка к сертификации и управление сертификацией объекта. Первый опыт уже есть: в конце января успешно прошли сертификационные испытания на соответствие требованиям Tier III Uptime Institute ЦОДа Key Point во Владивостоке.

– **А что представляет собой команда «Ди Си Квадрат»?**

– Старая гвардия со мной с 1999 г. Новые сотрудники – с конца прошлого года. Мы специфичная команда в плане подбора персонала и организации процесса работы. У нас нет офиса, мы работаем «от заказчика». Все сотрудники самоорганизованные, для них работа вне офиса – это нормально.

Почти все члены команды старше 40 лет. Это состоявшиеся профессионалы, которым никому ничего не надо доказывать. У них нет любимых технических решений или любимых производителей – они одинаково хорошо знают линейки разных вендоров, и мы подбираем оптимальный вариант для конкретной задачи.

– **Какие приоритеты на сегодня?**

– Проектов сегодня намного больше, чем людей. Поэтому первый приоритет – найти сотрудников с таким же высоким человеческим и профессиональным уровнем, как и у тех, что уже работают. Важно сохранить нашу командную атмосферу – всем очень комфортно, за 15 лет в коллективе не было ни одного конфликта, все всегда стараются помочь друг другу.

Второй приоритет – повышение сложности оказываемых услуг. Например, мы сейчас делаем для заказчиков расчеты по механическим и электрическим системам, их моделирование и т.д. В этой работе велика интеллектуальная составляющая, но важно и специализированное ПО. Поэтому надо поднять уровень инструментальной базы.

– **За какие проекты вы беретесь, а от каких отказываетесь?**

– Проект должен быть сопоставим с уровнем нашей команды. Привлекать нас в проект на 50 стоек, как правило, экономически неоправданно. Наши проекты в основном большие: сотни и тысячи стоек и мощность больше 10 МВт. Нередко это проекты сложные с точки зрения реализации: может потребоваться выполнить проект в очень короткий срок или площадка располагается в не слишком подходящих условиях.

Не беремся за проекты с длительными сроками от момента инициации до завершения. Хотя мы занимаемся консалтингом, но хотим видеть построенный объект. Не хочется входить в проект, где 1,5 года готовятся технико-эко-

номические обоснования, потом – процедуры закупок, в результате которых могут измениться условия задачи и потребуются заход на второй круг. Мы предпочитаем взять работу, выполнить ее максимально быстро и качественно и заняться следующей.

– **Как строятся ваши взаимоотношения с исполнителями работ (инженерными компаниями, системными интеграторами)?**

– Часто возникают жаркие производственные споры. Подрядчики привыкли, что заказчик принимает все, что они «нарисуют». А мы не принимаем. Нам нужно, чтобы у заказчика было лучшее решение. На посредственное мы не соглашаемся. Поэтому спорим, даже ругаемся, пока они не поймут, что придется делать как надо, а не как им хочется. Но бывает, что подрядчик изначально понимает правила игры и принимает их. Тогда все идет проще и быстрее.

Мы реализуем жесткий дополнительный контроль. По ряду разделов даже более жесткий, чем Uptime Institute. Проверяем все расчеты, подборы, боремся, чтобы исполнитель устранил недочеты. В результате проекты становятся лучше проработанными, несут меньше риска для заказчика.

– **А как работаете с производителями оборудования?**

– С вендорами мы в общем-то не работаем. У нас есть каталоги, мы наблюдали большую часть оборудования в эксплуатации, понимаем все плюсы и минусы.

Мы руководствуемся принципом vendor neutral. Многие вендоры делают прекрасные продукты, но любая привязка к конкретному производителю плоха. Важны взаимозаменяемость и итоговая коммерческая эффективность проекта.

Если вендор изначально понимает, что он получит проект, то он и напрягаться особенно не будет, и цен нормальных не даст. Только реальная конкуренция и осознание вендором того, что он может потерять проект, способны дать наилучшую стоимость. Управление ценой – еще одна услуга, которую мы оказываем.

– **Как вы видите текущую ситуацию на рынке? Каковы ваши планы?**

– Количество стоек быстро увеличивается, несмотря на то что рост тормозится проблемами с финансированием и с поставкой оборудования. Сегодня при высоких налогах и дорогих деньгах есть вопросы к окупаемости проектов. Стоек нам надо, конечно, гораздо больше, чем строится. Хотя наш проект Key Point (предусматривает строительство в регионах 35 ЦОДов общей емкостью 10,3 тыс. стойко-мест. – Прим. ред.) может улучшить ситуацию, но его одного явно недостаточно.

Если говорить о «Ди Си Квадрат», то я хочу выйти на международный рынок, начать оказывать консалтинговые услуги за пределами России. В первую очередь в странах бывшего СССР, в арабских странах. Уровень квалификации команды высок, наша инженерная школа уникальна, за рубежом таких специалистов почти нет. У «Ди Си Квадрат» большой потенциал. Будем наращивать команду и развивать новые рынки.



Key Point – крупнейший на Дальнем Востоке

В начале февраля 2023 г. резидент территории опережающего развития «Надеждинская» – компания Key Point – запустила в промышленную эксплуатацию первый на Дальнем Востоке и в Восточной Сибири коммерческий ЦОД международного уровня. Инвестиционный проект реализован по соглашению с Корпорацией развития Дальнего Востока и Арктики (КРДВиА) при финансовой поддержке ВЭБ.РФ.

Генеральный директор
Key Point Group
Александр Мартынюк



«Мы построили ЦОД в запланированный срок и прошли сертификацию международного института, подтвердив высокую надежность реализованного проекта».



Реклама

ЦОД Key Point емкостью 880 ИТ-стоек и мощностью 10 МВт, прошедший сертификацию Uptime Institute по уровню надежности Tier III, строится по модульной технологии в две очереди. Первая включает два технологических модуля общей емкостью 440 стоек со средним энергопотреблением 5 кВт.



Конструкция для имитации холодного коридора для испытаний Uptime Institute



Электрощитовая



Машинный зал



**Заместитель председателя ВЭБ.РФ
Артем Довлатов**

«Развитие информационной инфраструктуры создает задел для скорейшего внедрения на Дальнем Востоке принципиально новых и перспективных технологий и сервисов, таких как сети связи 5G, искусственный интеллект, беспилотный транспорт. Запуск дата-центра в Приморском крае повысит уровень доступности и устойчивости работы цифровых сервисов, а также будет способствовать улучшению инвестиционной привлекательности макрорегиона».

ЦОД международного уровня



**Генеральный директор
компании Key Point
Евгений Вирцер**

«Проект создания дата-центра Key Point во Владивостоке, безусловно, является вехой в развитии региональных ЦОДов в России, поскольку он реализован негосударственной компанией, но с поддержкой института развития и для решения в том числе государственных задач».



**Генеральный директор КРДВиА
Николай Запрыгаев**

«Мы рады, что статус резидента ТОР “Надеждинская” помог компании реализовать проект и повлияет на повышение качества услуг связи, интернета, цифровых сервисов не только для дальневосточников, но и для бизнеса».

Проект Key Point задолго до ввода в эксплуатацию вызвал живой интерес как у федеральных, так и у региональных компаний из разных отраслей. Ожидается, что до конца I квартала 2023 г. первая очередь ЦОДа будет законтрактована на 90%. Ввод в эксплуатацию второй очереди дата-центра – еще двух технологических модулей общей емкостью 440 стоек со средней мощностью 5 кВт – запланирован на I квартал 2024 г.



Системы автоматического газового пожаротушения (АГПТ)



Оборудование в помещении ИБП

Российские облака и платформы виртуализации: смена вендоров

Николай Носов

Системы виртуализации давно стали неотъемлемой частью бизнес-процессов. После ухода зарубежных вендоров, доминировавших на российском рынке, основные сценарии действий отечественных компаний – ждать, использовать привычное решение в облаке или перейти на российские продукты.

Поддерживать лучших

Санкции и уход с рынка зарубежных вендоров резко ускорили процессы импортозамещения в России, в том числе в области программного обеспечения. Выбор импортозамещающих продуктов облегчает Единый реестр российских программ для ЭВМ и баз данных (ЕРРП). Государство поддерживает решения из реестра с помощью преференций на конкурсах по госзакупкам и налоговых льгот, стимулирует создание экосистемы совместимых программных решений.

Решения постоянно развиваются, изменяются, и поддержка всех представленных в ЕРРП продуктов, например операционных систем, выглядит нерациональной тратой ресурсов. Но и ограничивать выбор одной операционной системой нельзя – это убьет конкуренцию на рынке ОС и приведет к стагнации продукта. Поэтому Минцифры предложило компромиссный вариант – опираясь на мнение бизнес-сообщества, выделить три-четыре наиболее зрелые российские операционные системы и обязать российских разработчиков обеспечивать совместимость с ними. Не соответствующие требованиям Минцифры продукты будут исключаться из реестра.

В будущем ограничения могут коснуться систем виртуализации и облачных платформ, число которых в ЕРРП перевалило за десяток. Во всяком случае обсуждения этого вопроса в Минцифры уже идут.

Основные виды виртуализации

Виртуализация – предоставление программными средствами набора вычислительных ресурсов или их логического объединения, абстрагированное от аппаратной реализации и обеспечивающее логическую изоляцию друг от друга вычислительных процессов, которые выполняются на одном физическом ресурсе. Основные преимущества виртуализации – повышение эффективности использования вычислительных ресурсов, легкость управления вычислительной средой и простота масштабирования ее элементов.

Виртуализация позволяет создавать независимые и изолированные друг от друга виртуальные объекты с помощью программной имитации физических ресурсов (процессора, памяти, сети, диска). Наиболее часто используется серверная виртуализация, когда на физическом сервере разворачиваются несколько виртуальных машин (Virtual Machine, VM). С серверной виртуализации началось проникновение технологии на рынок. Позже появились: виртуализация хранилищ данных – программно определяемые хранилища

(Software-Defined Storage); виртуализация сетей – виртуальные частные сети (Virtual Private Network, VPN) и программно определяемые сети (Software-Defined Network, SDN); гиперконвергентные системы (Hyper-Converged Infrastructure, HCI) – когда в виртуализированный масштабируемый стек объединяются серверы, СХД и сети. Пару лет назад появились программно определяемые территориально распределенные сети (SD-WAN).

Отделить логический рабочий стол (набор пользовательских программ, работающих под операционной системой) от физической инфраструктуры (например, ПК или сервера) позволяет виртуализация рабочих столов (Virtual Desktop Virtualization, VDI).

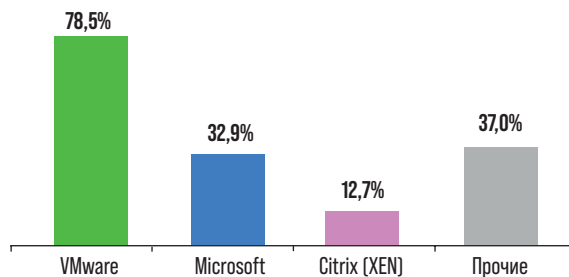
Все шире используется виртуализация операционной системы (контейнерная виртуализация), которая дает возможность запускать программное обеспечение в изолированных на уровне ОС пространствах. Наиболее распространенной формой виртуализации на уровне ОС являются контейнеры Docker, а системой управления – Kubernetes.

Наибольшее после операционных систем влияние на экосистему российских продуктов оказывает серверная виртуализация, которая выступает фундаментом и для построения облачных платформ. Упрощенно основными частями облачной платформы являются:

- гипервизор – аппаратная или программная система для параллельной работы на одном компьютере нескольких операционных систем, виртуализирующая аппаратные ресурсы для работы ОС;
- система, обеспечивающая динамическую балансировку нагрузки на серверы и системы хранения данных для повышения их производительности, поддерживающая высокую доступность виртуальных серверов, а также изоляцию виртуальных инфраструктур различных пользователей друг от друга на сетевом уровне;
- система управления виртуализацией, т.е. управления отдельными виртуальными машинами (создание, выделение ресурсов, доступ к консоли VM), комплексом взаимозависимых виртуальных машин, необходимых для реализации одного сервиса, а также виртуальными сетями и сетевым взаимодействием между машинами;
- система самообслуживания по требованию;
- система учета потребляемых ресурсов.

Первые три части можно объединить понятием «платформа виртуализации». Облачная платформа может поддерживать работу нескольких платформ виртуализации, в том числе с различающимися гипервизорами.

Рис. 1. ►
Использование платформ серверной виртуализации в России, процент опрошенных



Источник: опрос iKS-Consulting (2018 г.), респонденты могли назвать несколько платформ виртуализации

Рынок до и после начала СВО

Еще год назад на российском рынке средств виртуализации доминировали зарубежные, прежде всего американские компании (рис. 1), которые ушли с рынка после начала СВО на Украине, тем самым освободив пространство для российских игроков.

Соответственно наиболее популярными гипервизорами на российском рынке были ESXi от компании VMware и Hyper-V от Microsoft. Существенно уступали лидерам Xen от Citrix и VM VirtualBox, выкупленный Oracle у компании Sun. Среди open source-гипервизоров чаще всего использовался гипервизор KVM.

Облачные платформы на базе решений VMware стали практически стандартом в российском корпоративном секторе. Широкий набор продуктов для построения полноценного сервис-ориентированного частного, публично-гибридного облака предоставляет платформа для облачной инфраструктуры VMware Cloud Foundation (рис. 2), базирующаяся на гипервизоре VMware ESXi и платформе виртуализации VMware vSphere.

С помощью VMware Cloud Foundation можно создать полноценный программно определяемый

центр обработки данных (Software-Defined Data Center, SDDC), использовать продукт vSAN для гиперконвергентного хранилища, NSX – для виртуализации сетей. SDDC выступает системой управления виртуализации, vRealize обеспечивает мониторинг ресурсов и их производительности, учет потребляемых ресурсов, предоставляет каталог сервисов и портал самообслуживания. Опционально можно задействовать продукты для работы с современными приложениями семейства Tanzu и запускать контейнеры и кластеры параллельно с виртуальными машинами на той же инфраструктуре.

Среди облачных платформ с открытым исходным кодом наибольшую популярность завоевала OpenStack (рис. 3).

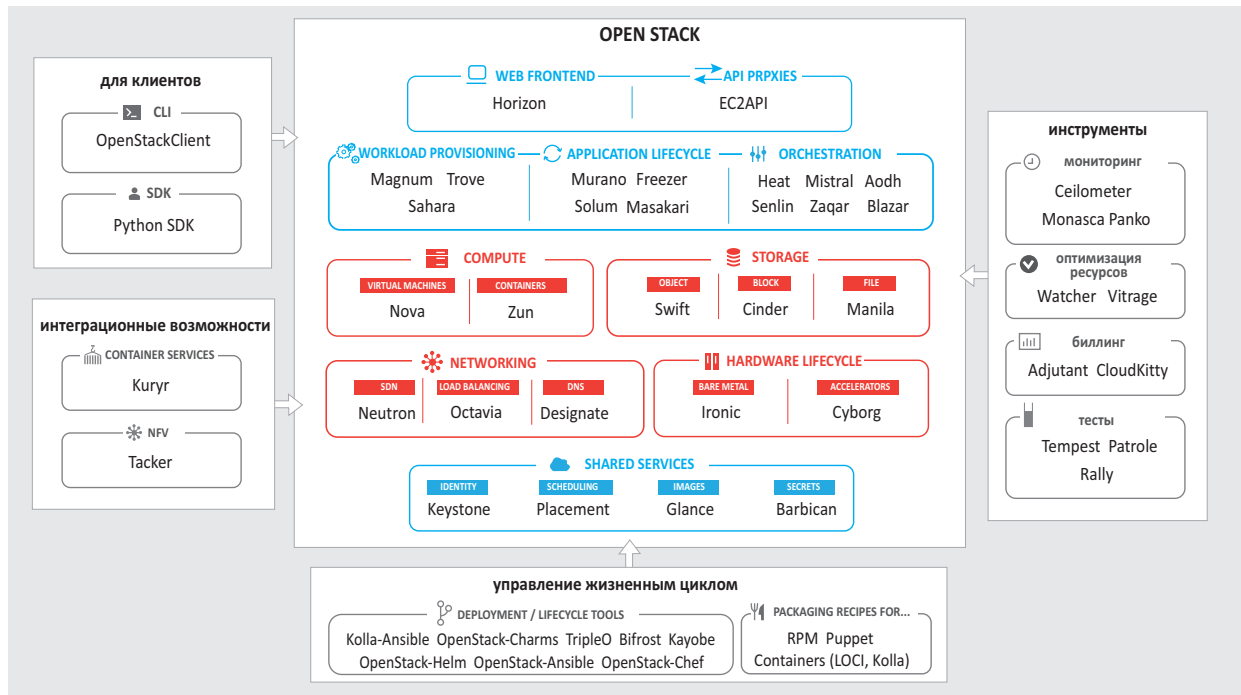
За серверную виртуализацию отвечает проект Nova. Для работы с хранилищами данных используются Cinder, Manila и Swift, виртуализацию сетей обеспечивают Neutron, Octavia и Designate, хранение образов виртуальных машин – Glance. Среди систем управления виртуализацией – каталог приложений с универсальным инструментарием для упрощения и ускорения упаковки и развертывания образов (проект Murano), системы автоматического восстановления отказавших виртуальных машин Masakari, автоматизации резервного копирования и восстановления данных Freezer, упрощения использования облачных сервисов и их интеграции в процесс разработки приложений Solum.

Среди других open source-платформ виртуализации стоит отметить OpenNebula и oVirt, поддерживаемые в основном компанией Red Hat. Из программно определяемых платформ хранения выделим Ceph.

Рис. 2. Продукты VMware Cloud Foundation ▼



Источник: VMware



◀ Рис. 3.
Экосистема
OpenStack

Источник:
Miro.medium.com

Выбор стратегии

Уход ведущих мировых вендоров заставил российские компании пересмотреть стратегии использования и развития информационных систем, в том числе в области виртуализации. Вариантов поведения в данной ситуации несколько.

1. Выжидательный – ничего не менять, ожидая, что зарубежные вендоры вернуться. Плюс – не нужно что-либо делать и тратить ресурсы. Минус – постоянно возрастающие технологические и юридические проблемы из-за окончания срока действия лицензий, отсутствия обновлений и техподдержки. В качестве временной меры можно задействовать нелицензионное ПО и искать техподдержку у российских интеграторов.
2. Переход на зарубежное решение в российское публичное облако. Многие российские облачные провайдеры имеют долгосрочные контракты с западными вендорами и в полном объеме предоставляют их услуги по сервисной модели. Минус – нужна перестройка процессов при миграции в облако. Для крупных организаций в долгосрочной перспективе публичные облака по экономике проигрывают модели on-premise, многие не могут использовать публичные облака из-за регуляторных требований.
3. Переход на самописное или open source-решение. Плюс – не надо платить сторонним организациям, минус – нужна своя команда разработчиков или как минимум хорошо разбирающихся в решениях open source инженеров. Вариант приемлем для крупных компаний, имеющих штат квалифицированных ИТ-специалистов.

4. Переход на кастомизированное российское проектное решение. Интересен в первую очередь крупным компаниям со сложными бизнес-процессами. Плюс – интегратор реализует все, в том числе специфические требования бизнеса. Минус – дорого на этапах разработки и внедрения, а также медленно, процесс может занять несколько лет.

5. Переход на российское продуктивное решение. Приемлемый вариант для малых и средних компаний – решение из коробки разворачивается быстро и без привлечения интеграторов. Минус – придется подстраивать бизнес-процессы под то, что предлагают.

6. Переход на российское продуктивное решение в российское же публичное облако. Отличный вариант для малых предприятий – не нужна экспертиза (которой, скорее всего, и нет) для развертывания и поддержки решения. Оплата – только за реальное использование сервиса. Минус – отсутствие кастомизации. Кроме того, при длительной эксплуатации затраты на облачный сервис превысят затраты на покупку ПО.

Последние три варианта предусматривают обращение к российскому ПО. Хуже всего ситуация с продуктовыми решениями, которые раньше с трудом выдерживали конкуренцию прежде всего с продукцией VMware. Лучше дела обстоят с кастомизированными проектными решениями, к которым крупные российские предприятия и раньше прибегали по экономическим и регуляторным причинам. Теперь российские вендоры, в том числе подразделения разработки крупных предприятий, выделенные в инсорсинговые компании, на базе проектных решений могут создавать «коробочные» продукты.

Российские платформы виртуализации: выбор есть

На рынке уже присутствуют российские решения, которые могут быть использованы для построения облачных платформ.

В Едином реестре российских программ для ЭВМ и баз данных (ЕРРП) представлен широкий спектр связанных с облачными вычислениями инфраструктурных решений, в том числе облачные платформы, программно определяемые каналы до них (SD-WAN), системы управления гибридными, связанными между собой технологиями передачи данных и приложений, частными и публичными облаками.

Российские облака, включающие модули учета потребляемых клиентами ресурсов и систему самообслуживания по требованию, могут иметь в своем составе решения контейнерной виртуализации и VDI (в публичном облаке DaaS, Desktop as a Service). Они могут быть развернуты на гиперконвергентной платформе, но чаще всего базируются на платформе серверной виртуализации.

Платформы серверной виртуализации

На рынке присутствует целый ряд российских платформ виртуализации, наиболее известные приведены в табл. 1. Их можно брать за основу при построении облачных платформ, дописывая недостающие модули или адаптируя уже существующие open source-компоненты.

Очевидно, что удобнее и надежнее работать с платформой, являющейся частью экосистемы решений разработчика, в которую входит и операционная система. Это сразу снимает вопросы о совместимости продуктов. Поэтому логично ориентироваться на наиболее известные отечественные ОС, которые с высокой вероятностью будут включены Минцифры в перечень перспективных и соответственно продолжат получать преференции и поддержку государства. К числу таких ОС

можно отнести Astra Linux («РусБИТех-Астра»), «Альт» («Базальт СПО») и «РЕД ОС» («РЕД СОФТ»). В случае попадания в список приоритетных они автоматически получают конкурентные преимущества и на рынке серверной виртуализации.

На ОС Astra Linux работает программный комплекс средств виртуализации «Брест» от ГК «Астра», который уже используется в качестве основы облачной платформы. Помимо наличия развитой экосистемы, конкурентное преимущество ПК СВ «Брест» – сертификация по самому высокому уровню защиты. По утверждению экспертов компании, это единственная система, работающая с высшими уровнями секретности без наложенных систем безопасности. В основе решения – элементы облачной платформы с открытым исходным кодом OpenNebula. Но если в «ванильной» (стандартной) версии OpenNebula сущности создаются администратором (root), то в «Бресте» каждая сущность внутри программного комплекса создается конкретным пользователем. За счет этого появляются дополнительные возможности ограничивать потребление ресурсов и отслеживать работу пользователя.

Базовый функционал виртуализации реализован в составе ОС с помощью гипервизора KVM, эмуляции аппаратного обеспечения QEMU, демона и набора инструментов для управления виртуализацией libvirt, приложения для управления виртуальными машинами virt-manager. Использование OpenNebula накладывает ограничения на масштабирование. Ряд экспертов считает, что эту облачную платформу не следует задействовать, если физических серверов более 30. Однако и это немало и, как правило, для создания частного облака вполне достаточно.

Российские программы виртуализации 2022 ▼



Решение востребовано в госструктурах с повышенными требованиями к защите информации. Наличие таких клиентов сильно повышает вероятность попадания в список приоритетных систем виртуализации.

С приобретением в 2022 г. компании «ИСП-систем» (ISPsystem) в портфеле ГК «Астра» появились коробочные решения из ЕРРП: BILLmanager, платформа автоматизации продаж и предоставления услуг IaaS, и VMmanager, платформа виртуализации on-premise, которую компания позиционирует как аналог VMware vCenter, VMware vCloud Director и VMware NSX. Совместная работа продуктов BILLmanager и VMmanager позволяет построить IaaS-хостинг под ключ.

Платформы виртуализации «РЕД Виртуализация» компании «РЕД СОФТ» и «Альт Сервер Виртуализации» от «Базальт СПО» пока не дотягивают до звания облачной платформы, но могут быть до нее доработаны. Минусом решения «РЕД СОФТ» с точки зрения импортозамещения можно считать основу – продукты американской компании Red Hat (прежде всего платформа oVirt), на что прямо намекает название «РЕД». Плюс – удобство работы и богатый дополнительный функционал, обусловленный поддержкой ИТ-гиганта. Впрочем, Северной Корее использование американских разработок с открытым исходным кодом не помешало провести импортозамещение ОС, разработав свою операционную систему Red Star – по сути пересобранную Red Hat Linux.

Платформа Veil и ее форк SpaceVM, появившийся после перехода части команды разработчиков НИИ «Масштаб» в новую компанию «ДАКОМ М», претендуют на то, чтобы называться облачными платформами, но по сути ими не являются, поскольку не имеют в своем составе систем учета и самообслуживания. Поэтому логично отнести их к платформам виртуализации.

Интеграция и миграция

Мало иметь свою платформу виртуализации, надо обеспечить клиенту возможность плавного перехода на новое решение, например, в частное или публичное облако с помощью гибридной инфраструктуры, включающей замещаемую импортную и российскую платформы виртуализации. Такая гибридная инфраструктура может быть и мультиклаудной. Российских систем для управления мульти- и гибридными облаками на рынке тоже несколько (табл. 2).

На работу с гибридными облаками ориентированы решения CloudMaster компании «СофтЛайн Платформы». Пользователи входящего в платформу CloudMaster мультиоблачного оркестратора Clouder могут из единой точки видеть все свои виртуальные машины, включая облако Yandex Cloud, самостоятельно разворачивать

Решение	Дата включения в ЕРРП, рег. номер	Компания-разработчик
«Рустэк»	01.06.2016, № 981	«Рустэк»
«Р-Виртуализация»	03.05.2017, № 3348	«Росплатформа»
ПК СВ «Брест»	23.07.2017, № 3742	«РусБИТех-Астра» (ГК «Астра»)
«Хост»	16.04.2018, № 4407	ГК «Хост»
SharxBase	16.04.2018, № 4445	«Шаркс Датацентр»
Veil	05.07.2018, № 4608	НИИ «Масштаб»
«Горизонт-BC23»	19.09.2018, № 4764	ИЦ «Баррикады»
zVirt	03.12.2018 № 4984	«Орион»
ROSA Virtualization	10.01.2019 № 5091	НТЦ ИТ РОСА
«Альт Сервер Виртуализации»	07.04.2020, № 6487	«Базальт СПО»
«РЕД Виртуализация»	01.09.2020, № 6929	«РЕД СОФТ»
«СКАЛА-Р Управление»	14.02.2022 № 12847	«Базис»
SpaceVM	29.12.2022, № 16085	«ДАКОМ М»

Источник: ЕРРП

виртуальные машины, создавать и редактировать их параметры в рамках предоставленных прав. Пользователи биллинга Coster смогут увидеть плановое, фактическое и прогнозное потребление облачных ресурсов, получат возможность управлять бюджетом.

Единую точку входа для запроса ресурсов на разных платформах, как on-premise, так и в облаке, предоставляет платформа управления мульти- и гибридными облаками «РОСА. Менеджер ресурсов» от НТЦ ИТ РОСА. Готовится заявка на включение этого решения в ЕРРП. Платформа поддерживает гипервизоры KVM и ESXi и упрощает миграцию с платформы VMware на российскую ROSA Virtualization. «Миграция с платформы VMware не одномоментный процесс, и у заказчика будут две платформы виртуализации, которыми нужно будет управлять. Упростит процесс система автоматизации работы с различными платформами виртуализации «РОСА. Менеджер ресурсов», которая собирает информацию об используемых ресурсах и проводит биллинг. Платформа работает в режиме multitenancy, и ее может задействовать облачный провайдер для предоставления сервисов. Например, дата-центр холдинга будет оказывать услуги для входящих в него предприятий. Платформа поддерживает гибридный режим работы – в мае 2023 г. выйдет версия, поддерживающая работу с Yandex Cloud. В дальнейшем будут подключаться другие российские публичные обла-

▲ Табл. 1. Наиболее известные российские платформы серверной виртуализации

Табл. 2. Российские системы управления гибридными облаками и мультиклаудом ▼

Решение	Дата включения в ЕРРП, рег. номер	Компания-разработчик
Платформа Velvica	03.05.2017, № 3411	«Велвика» (ГК Merlion)
CloudMaster	14.12.2020, № 7846	«СофтЛайн Платформы»
«РОСА. Менеджер ресурсов»	–	НТЦ ИТ РОСА

Источник: ЕРРП

ка», – рассказал нашему изданию генеральный директор НТЦ ИТ РОСА Олег Карпицкий.

Мультиклауд на уровне биллинга обеспечивает входящая в контур проекта MerlionTech платформа Velvica от компании «Велвика». Решение позволяет полностью автоматизировать бизнес-процессы, связанные с продажей облачных сервисов.

Гиперконвергентные платформы

Простота управления и эксплуатации, снижение расходов на поддержку ИТ-инфраструктуры, легкость масштабирования – основные преимущества гиперконвергентных решений, которые объединяют на программном уровне диски и дисковые полки серверов и интегрированных блоков с помощью развернутой на них платформы виртуализации. С точки зрения наращивания вычислительных мощностей получающаяся гиперконвергентная инфраструктура (Hyper-Converged Infrastructure, HCI) уже не ограничена возможностями одного интегрированного модуля устройства или сервера – платформа объединяет их ресурсы в единое целое, из которого можно «нарезать» нужные для конкретной задачи вычислительные мощности.

Российские аналоги используемых на нашем рынке продуктов Nutanix и VMware (решение становится гиперконвергентным, когда на VMware vSphere/vCloud «надевается» vSAN) – продукты компании «Росплатформа» («Р-Виртуализация» и «Р-Хранилище»), гиперконвергентная инфраструктура vStack компании ITglobal.com («Итглобалком Рус») и vAIR, разработанный НИЦ «Аэродиск» (табл. 3). Гиперконвергентный функционал есть и в платформе ROSA Virtualization, построенной на базе open source-продукта компании Red Hat.

Достоинство продуктов «Росплатформы» – узнаваемость на рынке и большое количество внедрений, прежде всего в государственных и связанных с государством структурах. «Под управлением ПО “Росплатформы” в режиме промышленной эксплуатации у российских заказчиков работает более 3000 CPU и хранилища объемом 7500 Тбайт. В продукте “Р-Виртуализация” используется гипервизор на базе QEMU/KVM и libvirt. Вопреки бытующему на рынке мнению, “Р-Хранилище” не базируется на Ceph, а является распределенным хранилищем промышленного уровня, самостоятельно разработанным с нуля. Для контейнерной виртуализации служит

OpenVZ, а популярный Docker/Kubernetes можно вставлять внутрь контейнеров “Росплатформы”. Платформу можно использовать для построения частного облака, но с ограничением функциональности портала самообслуживания. Каких-либо “коробочных” интеграций с порталами самообслуживания для продуктов “Росплатформы” на данный момент не существует, поскольку подходы к построению облака у всех разные», – сообщил управляющий директор «Росплатформы» Сергей Члек.

Преимущества vAIR от «Аэродиска» – простота и возможность использования решения «из коробки». Компания успешно внедряла open source-решения для организации растянутого хранилища (Ceph, GlusterFS, Lustre), но это были проектные решения для конкретных заказчиков. Самостоятельно разработанный компанией продукт vAIR позиционируется как массовый, способный разворачиваться и работать без поддержки вендора.

Свое гиперконвергентное решение vStack компания ITglobal.com смогла поднять до уровня полноценной облачной платформы. В состав входят vStack SDN (программно определяемый слой сети), vStack SDC (вычислительный слой), vStack SDS (слой хранения данных), vStack Management (компонент управления слоями) и vStack OS – слой взаимодействия ПО и оборудования. В основе технологический стек из операционной системы FreeBSD, гипервизора vStack (на базе гипервизора bhyve) и файловой системы ZFS, обеспечивающий, по утверждению разработчиков, более высокую производительность, чем классическая связка гипервизора KVM и OpenStack или менее распространенная OpenNebula и oVirt. Решение позволяет строить производительные облачные системы. Показатель CPU overcommit (выделение суммарного количества процессоров, превышающего общее количество логических процессоров на хосте) в продуктовых инсталляциях достигает 900%. Частное или публичное облако разворачивается по проектной модели для конкретного заказчика. Есть биллинг.

На российском рынке vStack стали рекламировать только в последнее время, хотя сама ITglobal.com работает давно: до продажи в конце 2018 г. своего облачного бизнеса МТС она носила название «ИТ-Град». В январе 2022 г. компания сообщила о приобретении облачного гиперскелера Serverspace, присутствующего на рынках США, Канады, Нидерландов, стран СНГ и Азии.

Заказчики могут воспользоваться всеми услугами, предоставляемыми облачным провайдером в регионе, а также применять гибридную модель при построении ИТ-инфраструктуры. «Компания Serverspace задействует платформу vStack для предоставления клиентам услуг

Табл. 3. Российские гиперконвергентные платформы ▼

Решение	Дата включения в ЕРРП, рег. номер	Компания-разработчик
«Р-Хранилище»	03.05.2017, №3380	«Росплатформа»
ROSA Virtualization	10.01.2019, № 5091	НТЦ ИТ РОСА
vAIR	31.12.2020, №8802	НИЦ «Аэродиск»
vStack	18.11.2021, №11995	ITglobal.com («Итглобалком Рус»)

Источник: ЕРРП

IaaS – создания клиентских виртуальных дата-центров и виртуальных машин/сетей внутри этих дата-центров. Платформа используется наряду с платформой виртуализации VMware, и клиенты Serverspace сами решают, какую платформу им выбрать», – сообщил основатель ITglobal.com Дмитрий Гачко.

Гиперконвергенция позволяет перейти от вертикального масштабирования к горизонтальному, хорошо подходит там, где нагрузка идет не «вглубь», а «вширь»: для масштабирования стандартных инфраструктурных сервисов (файловые серверы, почта и т.п.), VDI, распределенных вычислений, включая сервисы Big Data.

Российские облачные платформы: гамбургский счет

Технические характеристики, наличие внедрений, якорные клиенты, квалификация команды разработчиков, узнаваемость бренда – вот критерии выбора облачной платформы.

Существующие решения

Целый ряд стратегий поведения российских компаний после ухода с рынка ведущих зарубежных вендоров предусматривает переход на отечественные облачные платформы. Таковые широко представлены в Едином реестре российских программ для ЭВМ и баз данных (ЕРПП). Отфильтруем решения в реестре по основному коду 02.03 («Средства обеспечения облачных и распределенных вычислений») классификатора ПО, утвержденного приказом Минцифры России от 22.09.2020 № 486. Добавим решения с кодом 02.05

(«Средства обеспечения облачных и распределенных вычислений, средства виртуализации и системы хранения данных») из более старого, но еще действующего классификатора, утвержденного приказом от 31.12.2015 № 621. К ним добавим «Облачную платформу ВТБ» (VTB Cloud), по непонятной причине попавшую в классификатор с другим кодом. Оставим для рассмотрения только предлагаемые на рынке инфраструктурные облачные платформы, имеющие известные внедрения, с учетом прошедших слияний, поглощений и переименований (табл. 1).

Табл. 1. Российские облачные платформы ▼

Решение	Дата включения в ЕРПП, рег. номер	Компания-разработчик	Гипервизор	Платформа	Облако
ПК СВ «Брест», BILLmanager, VMmanager	23.07.2017, № 3742 14.06.2016, № 1184 16.05.2016, № 790	«РусБИТех-Астра» (ГК «Астра»)	KVM	OpenNebula	Частное облако для крупных предприятий
«Базис.DynamiX»	06.05.2019, № 5379	«Базис»	KVM	Собственная разработка	Публичное и частное
«Облачная платформа КРОК»	06.05.2019, № 5386	КРОК	KVM	Собственная разработка	«Коммунальное» и частное
Private Cloud от VK*	13.01.2020, № 6092	«VK Цифровые технологии»	KVM	OpenStack	Публичное и частное
Rustack Cloud Platform**	09.06.2020, №6672	«Рустэк»	KVM	OpenStack	Публичное и частное
Yandex Cloud	20.02.2021 № 9286	«Яндекс»	KVM	Собственная разработка (ранее – OpenStack)	Публичное
«Облачная платформа Сбербанка» (Platform V)	30.12.2020 №8500	«Сбертех»	KVM	OpenStack	Частное
«Базис. Cloud» (Tionix Cloud Platform)***	31.12.2020 № 8740	«Базис»	KVM	OpenStack	Частное
«Облачная платформа Selectel»	25.03.2021, № 9884	Selectel	KVM	OpenStack	Публичное
VTB Cloud	22.10.2021 №11873	ВТБ	KVM	OpenStack	Частное
vStack	18.11.2021 №11995	ITglobal.com («Итглобалком Рус»)	bhyve	oVirt	Публичное и частное
Rockit Cloud («Рокит Клауд»)	23.12.2022 №16035	«Рокитсофт» (ранее «КРОК регионы»)	KVM	Собственная разработка	Частное

* Также в ЕРПП включено «Облако Mail.ru» (21.04.2021, № 10379) от VK

** Комплекс оркестратора «Рустэк – Единая система управления» и платформы виртуализации «Рустэк»

*** Также в ЕРПП включена Tionix Cloud Management Platform (15.04.2022, № 13310) от «Тионикс».

Источник: ЕРПП

Видим, что список достаточно обширен. Минцифры заявило о намерении выбрать в реестре сильнейшие решения и консолидировать вокруг них другие активы (т.е. требовать совместимости с выбранными) с целью более эффективного использования средств. На первом этапе речь пойдет об операционных системах, в перспективе селекция может коснуться и средств виртуализации и облачных платформ. Вопрос выбора волнует и заказчиков, опасаящихся «поставить не на ту лошадь» и потерять инвестиции. Попробуем разобраться с критериями, исходя из которых можно отдать предпочтение той или иной системе.

Российские облачные платформы построены на решениях open source. «Под капотом» почти всех импортозамещающих платформ виртуализации – гипервизор KVM. Лишь одна vStack базируется на bhyve. По утверждению компании ITglobal.com, за счет использования bhyve повышается производительность облачной платформы. Но конкуренты с этим не согласны, справедливо требуя результатов тестирования независимыми экспертами. Если же смотреть по числу внедрений, доля использования KVM будет еще выше. В публичных внедрениях разработок российских компаний bhyve используется только одним облачным провайдером.

Подавляющее большинство инфраструктурных (предоставляющих IaaS-сервисы) облачных платформ основывается на OpenStack, в качестве программно определяемого хранилища чаще всего используется Ceph.

Но помимо технологических параметров, есть важные различия, которые нужно учесть при выборе. В их числе – авторитет компании, востребованность решения на рынке и наличие внедрений на значимых объектах, квалификация разработчиков, встроенность в экосистемы и функциональные возможности, независимость от внешних игроков.

Якорные клиенты

Важный – а для государства, скорее всего, определяющий – критерий выбора облачной платформы – это наличие внедрений (табл. 2), прежде всего в государственных и окологосударственных структурах и на значимых объектах КИИ. Если платформа уже развернута и успешно используется, то менять ее без крайней необходимости нецелесообразно.

Впечатляет список внедрений входящих в платформу облачных продуктов компании «Базис» (ранее СП «Облачная платформа», одним из создателей которого является «Ростелеком»). В дополнение к этому в 2022 г. «Ростелеком» был назначен исполнителем работ по созданию ГИС «Единая централизованная цифровая платформа в социальной сфере» (первая очередь). Эта платформа будет использоваться в проекте «Социальное казначейство», который должен объединить ключевые социальные сервисы, реализовав принцип «одного окна», упростить выплату пособий, пенсий и социальных надбавок и автоматизировать процесс их начисления.

Используется у государственных заказчиков и удовлетворяющая повышенным требованиям безопасности облачная платформа компании «РусБИТех-Астра». Понятно, что на безопасности государство не экономит, особенно в сегодняшних сложных геополитических условиях.

У платформы компании «Рустэк» тоже есть достаточно масштабные внедрения: в облаке «Айтеко Cloud» (ранее «СБКлауд») под ее управлением работает более 60 физических серверов.

По числу внедрений остальные российские облачные платформы сильно уступают лидерам, хотя зачастую и имеют важных заказчиков.

Использование в публичных облаках

Публичное облако – наиболее сложный вариант задействования облачной платформы. Ведь кроме учета ресурсов надо иметь биллинг, причем такой, который позволял бы решать спорные вопросы по оплате в суде. Повышены по

Табл. 2. Наиболее известные внедрения российских облачных платформ ▼

Решение	Компания-разработчик	Внедрения
«Базис.vCore» «Базис.DynamiX» «Базис.Digital Energy» «Базис.WorkPlace» «Базис.Virtual Security» «Базис.WorkPlace Security»	«Базис» (СП «Облачная платформа»)	«Ростелеком», «Росатом», КНС Групп (Yadro), НПП «Исток», инфраструктура электронного правительства, ГЕОП, ФНС, Центризбирком, Федеральная кадастровая палата, Минтруд России, ГБ МСЭ по Еврейской АО, ГАУ СО ЦТЗ, ДИТ Москвы, Фонд социального страхования, Роспотребнадзор, «Ростех», Почта России, Газпромбанк
ПК СВ «Брест», BILLmanager, VMmanager	«РусБИТех-Астра» (ГК «Астра»)	«Росэнергоатом», НИКИЭТ, Росгеология, «Газпром трансгаз», администрации городов Магнитогорск и Северск (Томская обл.), Минцифры Челябинской обл.
Rustack Cloud Platform	«Рустэк»	«Ростех», АСВ, РЖД, «Айтеко Cloud», Cloud4y, Stack Group (M1Cloud), НИЯУ МИФИ, Makecloud.ru, MerlionCloud, Latt Telecom

Источник: данные компаний

сравнению с частным облаком и требования к безопасности клиентов, среди которых могут оказаться и злоумышленники, например, пытающиеся атаковать через гипервизор соседей по облаку. Да и самих пользователей больше, и нагрузка на платформу выше.

Поэтому уже само использование платформы в публичном облаке (табл. 3) много говорит о ее надежности и безопасности, использование несколькими провайдерами – о наличии рыночного решения.

По пути VMware – создания коробочного продукта для частных облаков и облачных провайдеров – дальше всех продвинулась компания «Рустэк», чья продукция используется четырьмя внешними провайдерами. Впрочем, на фоне числа внедрений мирового лидера и этот результат смотрится более чем скромно. Остальные российские разработчики идут или по пути AWS («Яндекс», Selectel), создавая облака для себя, или по пути Microsoft – для себя и для рынка, но успехи пока невелики.

По числу развернутых на облачной платформе сервисов лидируют «Яндекс», VK и Selectel.

Команда разработчиков

Большинство отечественных вендоров облачных платформ используют стандартные версии open source-продуктов, по сути добавляя лишь логотип своей компании. В этом есть риск – российские компании вынуждены потреблять то, что есть, и не могут влиять на развитие продукта. С другой стороны, собственная разработка несет риски зависимости от своих программистов, которые могут покинуть компанию. Оптимальный вариант – команда разработчиков, глубоко разбирающихся в open source-продукте и способных влиять на его развитие. Тогда в случае их ухода компания сможет опереться на международное комьюнити.

Грубо оценить уровень разработчиков можно по числу изменений (коммитов), внесенных в open source-проект. В большинстве случаев в

Число использований	Облачная платформа	Облачный провайдер	Вид и сервисы
4	«Рустэк»	«Айтеко Cloud», MerlionCloud, Cloud4y, Stack Group (M1Cloud)	Внешнее – публичное. IaaS, PaaS, SaaS
1	Yandex Cloud	Yandex Cloud	Свое – частное, внешнее – публичное. IaaS, PaaS, SaaS
1	VK Cloud (Private Cloud от VK)	VK Cloud	Свое – частное, внешнее – публичное. IaaS, PaaS, SaaS
1	«Облачная платформа Selectel»	Selectel	Свое – частное, внешнее – публичное. IaaS, PaaS, SaaS
1	vStack	Serverspace	IaaS

Источник: данные компаний

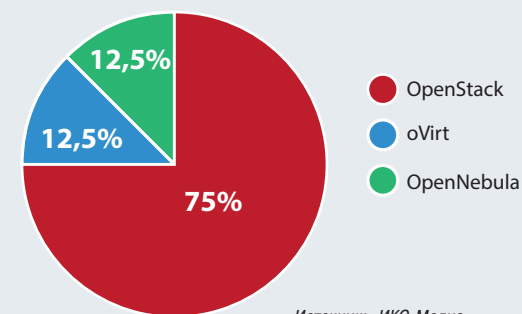
качестве облачной платформы с открытым исходным кодом используется OpenStack (см. рисунки). Отметим, что эту платформу в качестве замещающей западные разработки выбрали и крупнейшие китайские компании Huawei и Alibaba, сделавшие соответствующие форки Huawei Cloud и Alibaba Cloud.

Как свидетельствует сервис Stackalytics, собирающий данные о деятельности разработчиков, по числу коммитов в облачном проекте OpenStack с большим отрывом лидирует команда «Рустэк» – в совокупности 244 коммита (компания «Рустэк» появилась в результате консолидации ГК «Айтеко» в одном вендоре разработчиков компаний «Сервионика» и «СБКлауд»). Дальше идет плотная группа, которую составляют ВТБ (50), Сбербанк (46) и Selectel (38) (табл. 4).

Сходная картина и в объединившем инфраструктурные решения с открытым исходным кодом проекте OpenInfra. В тройке лидеров – снова «Рустэк», Сбербанк и ВТБ.

«Мы берем решение open source и пересобираем его. Даже ядро операционной системы у нас собственной сборки, что сильно повышает бы-

▲ Табл. 3. Использование российских облачных платформ в публичных облаках



◀ Использование в России облачных платформ с открытым исходным кодом

Табл. 4. ► Количество коммитов российских разработчиков в open source-проекты

Компания-разработчик	OpenStack	OpenInfra	Другие проекты
Servionica («Сервионика»)	180	201	21
SBCloud («СБКлауд»)	64	70	6
VTB (ВТБ)	50	80	30
Sberbank (Сбербанк)	46	78	32
Selectel	38	43	5
Mail.ru	12	16	4
Yandex («Яндекс»)	4	6	2

Источник: Stackalytics

стродействие. Мы не берем из OpenStack все модули, которые не всегда нужны, и дописываем то, чего не хватает, например, свой портал управления. У нас не просто платформа виртуализации, а платформа виртуализации плюс платформа оркестрации, способная управлять разными гипервизорами. За счет этого можно строить и частные, и публичные облака. И еще есть свой VDI. Три наших продукта позволяют удовлетворить все потребности заказчика в управлении ИТ-инфраструктурой», – дал комментарий нашему изданию генеральный директор «Рустэк» Георгий Мегрелишвили.

В 2022 г. компания перестроила бизнес-модель и, подобно VMware, стала заниматься только разработкой продукта, переложив продажи на дистрибьюторов и партнеров. Крупнейшие дистрибьюторы России – Axoft, Mont, Merlion, «Марвел-Дистрибуция», Treolan – не только продают «коробки», но развернули лаборатории и обучают партнеров, раньше продававших продукты VMware, внедрять продукцию «Рустэк» у клиентов.

«Для референсной архитектуры OpenStack характерно ограничение – 150–200 серверов, дальше надо создавать нетиповую архитектуру», – пояснил амбассадор OpenStack Илья Алексеев. Экспертизой по созданию архитектуры в тысячи серверов обладает ИТ-команда Сбербанка, точнее, его дочерней инсорсинговой компании «Сбертех». Она активно рекламирует свою облачную платформу Platform V. Квалификация разработчиков Сбера сомнений не вызывает, но рыночный продукт – это не только разработка. О внедрении платформы за пределами Сбербанка не слышно, и о рыночных перспективах платформы пока говорить рано.

Часть команды Сбербанка перешла в дочку ВТБ – компанию Т1 (ранее «Техносерв»), которая делает платформу VTB Cloud, похожую на платформу Сбербанка. Платформа еще не вышла на широкий рынок, но уже продается заказчикам группы ВТБ. Им предлагается создать частное облако или гибридное с корпоративным Т1 Cloud. ВТБ – одна из немногих российских компаний, продолжающих вносить коммиты в OpenStack после начала СВО.

Одной из первых в стране разработала (на базе OpenStack) свою облачную платформу для управления виртуальными центрами обработки данных компания «Тионикс», созданная в Казани и затем купленная «Ростелекомом». Весной 2022 г. путем объединения продуктовых линеек и команд разработки компаний «Тионикс», Digital Energy и «Скала Софтвр» было создано совместное предприятие «Облачная платформа» (ныне компания «Базис»). Компания рассчитывает за два года стать лидером в

сегменте государственных организаций и получить значительную (до 40%) долю в корпоративном секторе. Если учесть поддержку «Ростелекома», задача представляется вполне выполнимой.

Один из признаков сильной команды – эксплуатация созданной ею платформы в режиме публичного облака, когда инфраструктуру одновременно нагружают тысячи заказчиков. Такая команда есть у VK Cloud (поглотившей Mail.ru Cloud Solutions с решением «Облако Mail.ru»). Сейчас она пытается свое публичное облако «приземлить» on-premise. У всех перечисленных компаний неплохо обстоит дело с разработкой, и они могут попытаться занять нишу коробочных решений платформ виртуализации, освободившуюся после ухода VMware с российского рынка.

Самые популярные

Первое место по популярности облачных решений на официальном маркетплейсе «Руссофта» и Минцифры на момент написания статьи занимала «Облачная платформа КРОК», находящаяся в ЕРПП более трех лет. Компания предоставляет и публичное облако, и проектное решение для построения частного облака – для тех случаев, когда у заказчика есть регуляторные ограничения на использование публичных облаков, а также когда публичных облаков недостаточно и требуется кастомизированное решение.



Поскольку частное облако – это проектное решение, а не коробочное, возможности его широкого применения сильно ограничены, и внедрение облачной платформы – только половина задачи. Также нужно перестраивать бизнес-процессы, на что уходит минимум два года.

Публичное облако КРОК для предоставления услуг использует три зоны доступности (т.е. три независимых дата-центра). Такое количество ЦОДов позволяет строить катастрофически устойчивые кластеры, и это одно из преимуществ облачного решения КРОК по сравнению с облаками, работающими с одной зоной доступности. Другое преимущество – гарантированная производительность дисков. Клиент может получить до 50 000 IOPS на диск, за что провайдер несет ответственность, зафиксированную в соглашении о качестве услуг. С учетом текуще-

го тренда ИТ на повсеместную автоматизацию можно также выделить наличие собственного Terraform-провайдера и в целом мощного API для управления ресурсами из облака. Другим конкурентным преимуществом компания считает широкий спектр удобных, надежных сервисов PaaS: начиная от Kubernetes (кластер на три дата-центра разворачивается за несколько кликов) до разнообразных баз данных (MySQL, PostgreSQL, Redis, MongoDB), сервисов кеширования (Memcached, Redis) и сервиса для поиска, анализа и мониторинга данных Elasticsearch. Хотя облако КРОК позиционируется как публичное, но самостоятельно, «с улицы», зарегистрироваться нельзя. Организации могут оставить заявку на подключение. Поэтому облако КРОК вернее называть не публичным, а «коммунальным».

Многие предприятия и организации используют продукты, входящие в облачную платформу компании «Базис» (см. табл. 2). Задействуя облачную платформу для виртуализации серверов и систем хранения данных, можно обойтись без Microsoft Hyper-V и VMware vSphere. Разработанный на базе KVM гипервизор «Базис.vCore» заменит VMware ESXi. 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.

Узнаваемость зонтичного бренда

Популярность на официальном маркетплейсе «Руссофта» и Минцифры – критерий не слишком понятный. На основании чего она определяется, на самом маркетплейсе не поясняется. Да и большая часть российских облачных платформ там не представлена. Для потенциальных клиентов важнее узнаваемость зонтичного бренда облачной платформы, пусть даже известного по другим сервисам. Такую узнаваемость можно попробовать оценить по числу запросов по названию и частоте упоминания в интернете.

По статистике запросов в поиске «Яндекса» (табл. 5) на конец февраля 2023 г. ожидаемо лидировал бренд «Яндекс» (41 млн), на втором месте – VK (32 млн).

«Яндекс», VK и Selectel предоставляют сервисы из публичных облаков, поэтому узнаваемость бренда для них особенно важна. Причем VK предлагает свою облачную платформу не

Бренд	Количество запросов в России в феврале 2023 г.
«Яндекс»	41 млн
VK	32 млн
КРОК	13 млн
«Базис»	10 млн
«Рустэк»	3 млн
Selectel	92 тыс.

◀ Табл. 5.
Популярность зонтичных облачных брендов

только как сервис, но и как продукт, с помощью которого заказчики смогут создавать свои облака. У Selectel тоже готово решение для подобного применения – частное облако Selectel на базе OpenStack, функционирующее на оборудовании клиента (в собственном дата-центре или на базе услуги colocation) или арендованном у провайдера. Но оно еще не вышло на рынок.

В новой реальности

До начала СВО и ухода зарубежных вендоров на российском рынке серверной виртуализации и виртуализации систем хранения доминировали западные компании, прежде всего американская VMware. В стране много специалистов, привыкших работать с их решениями. Многие компании будут продолжать использовать зарубежные продукты, несмотря на отсутствие технической поддержки.

Для крупного бизнеса наличие квалифицированной поддержки принципиально, и компании рано или поздно начнут использовать отечественные продукты. Как показывает анализ ЕРРП, в России достаточно много разработчиков, которые накопили экспертизу, поставляя свои решения госсектору и попавшим под санкции компаниям. Российские вендоры ПО постараются удержать имеющуюся клиентскую базу и будут бороться за клиентов, у которых заканчиваются лицензии западных производителей.

В настоящее время на российском рынке среди отечественных вендоров явных лидеров нет, нет доминирующих игроков. Однако активно идут процессы консолидации, например, крупные российские разработчики объединились под брендом «Базис», а ISPsystem вошла в ГК «Астра», что существенно увеличило возможности группы на рынке облачных платформ.

Российские вендоры систем виртуализации смогут заместить ушедших западных вендоров, хотя для занимающихся импортозамещением компаний процесс будет болезненным вследствие инертности персонала, изменения интерфейса и отсутствия в новом ПО ряда уже ставших привычными функций. Борьба за освободившиеся ниши только начинается. ИКС

Новая страница истории GreenBushDC

Вхождение в состав группы компаний МТС и получение сертификата Tier III Facility дали новый импульс развитию ЦОДа GreenBushDC. На наши вопросы отвечает его генеральный директор Сергей Рубцов.



– Последние несколько лет были непростыми для экономики страны. Но отрасль ЦОДов продолжает устойчиво расти. Какие отраслевые тенденции вы бы выделили? Каким стал 2022 г. для GreenBushDC?

– Устойчивый рост рынка ЦОДов начался не сегодня. Он наблюдается уже много лет. Затем пандемия стала дополнительным драйвером развития ИТ-отрасли не только в России, но и во всем мире. Она привела к существенному росту спроса на онлайн-сервисы, что, естественно, потребовало увеличения ресурсов дата-центров. Конечно, сказались и трудности с логистикой, нехватка чипов.

Последние социально-политические события также оказали влияние на отрасль. С одной стороны, негативное – усложнился доступ к современным технологиям. С другой – позитивное: часть клиентов начала переносить свои системы из-за рубежа в Россию, вырос спрос на услуги коммерческих ЦОДов. Но есть задержки с вводом новых площадок, что обусловлено увеличением сроков поставки технологического оборудования в Россию. Поэтому имевшийся в Москве дефицит стойко-мест сохраняется.

Если говорить про GreenBushDC, то для нас год был насыщен событиями. Мы доработали наши серверные залы, в частности, построили современную систему распределения электроэнергии на базе шинопроводов. Также построили несколько ВОЛС, улучшив связность ЦОДа. Были организованы две новые ВОЛС: до М9 и соединение с магистральной сетью МТС. Сейчас строится еще одна линия – до М10. Наконец, самое главное, провели сертификацию ЦОДа на соответствие Tier III Facility от Uptime Institute, убедились, что надежность объекта соответствует самым высоким мировым требованиям.

– Вы упомянули дефицит площадей в большинстве московских ЦОДов. А какова ситуация у вас?

– У нас ситуация иная. Она обусловлена тем, что до завершения сертификации мы старались не привлекать в ЦОД «тяжелых» клиентов, дабы снизить риск их отключения в процессе сертификации. Сейчас у нас уникальное предложение на рынке: клиентам для размещения оборудования доступны четыре зала мощностью по 500 кВт. Суммарно 2 МВт. Таких объемов сейчас в Москве практически нет.

– А если перевести в стойки?

– Если считать в стандартных пятикиловаттных стойках, то это 100 стоек на зал, если в десятикиловаттных – 50 стоек. Наша инженерная инфраструктура позволяет устанавливать и более мощные стойки, до 20 кВт. Но полагаю более коррект-

ным оценивать емкость ЦОДа, исходя из мощности. Как правило, этот ресурс заканчивается быстрее, чем площадь.

– Ваш ЦОД прошел долгий путь сертификации на соответствие Tier III. Чем были вызваны сложности?

– Старт строительства ЦОДа GreenBushDC относится к началу 10-х годов. Сертификат на проект (Tier III Design) был получен в 2015 г. Но всем этим занимался предыдущий владелец. В 2021 г. ЦОД был куплен группой компаний МТС, и мы начали изучать состояние нового актива. В том же году провели испытания всех инженерных систем, проверили их готовность к сертификации. Весной 2022 г. совместно с экспертами Uptime Institute провели сертификацию. Да, нам потребовалось некоторое время, чтобы убедиться, что инфраструктура ЦОДа соответствует высоким требованиям МТС и Uptime Institute и что мы сможем гарантировать необходимый клиентам SLA.

Считаю, это даже хорошо, что сертификацию провели мы сами, а не предыдущий владелец. Это позволило нам убедиться, что все работает должным образом, дало возможность провести тренировку команды эксплуатации при работе объекта в автономном режиме. Да и для клиентов новый сертификат более убедителен, чем если бы он был получен предыдущим собственником.

В свое время по рынку ходило множество слухов, связанных с GreenBushDC. Безусловно, мы о них тоже знали и перед покупкой внимательно проанализировали возможные проблемы. Большая часть слухов не подтвердилась, а некоторые действительно имевшие место проблемы мы успешно решили.

Например, говорили о плохой связности: дескать, у ЦОДа всего один линк. Судите сами. Сегодня на площадке присутствуют семь телеком-операторов, до основных точек обмена трафиком проложены шесть ВОЛС по географически разнесенным маршрутам. Дополнительные вновь построенные ВОЛС имеют емкость по 128 волокон, а значит, подключать клиентов мы можем целыми волокнами. Наконец, имеется высокоскоростное подключение к сети МТС с ее практически неограниченными ресурсами магистральной связности по всей России.

Еще говорили о низкой нагрузочной способности перекрытий. Мы перед покупкой провели детальное обследование, в том числе с бурением, и убедились, что перекрытия способны выдержать 1250 кг на кв. м, что соответствует требованиям Uptime Institute.

– Традиционно большинство коммерческих ЦОДов в Москве строились в пределах МКАД. ЦОД Green-

BushDC находится за МКАД. В чем преимущества (и недостатки – если есть) такого расположения?

– Большинство ЦОДов, расположенных в Москве, испытывают серьезные трудности с подключением к электросетям. Так сложилось, что все ресурсы для подключения столь энергоемких объектов, как ЦОДы, уже исчерпаны. Кроме того, возникают вопросы с нецелевым использованием земельных участков и т.п. Наш ЦОД находится в Зеленограде, на территории ОЭЗ «Алабушево». Земля у нас в собственности, целевое использование подтверждено, общая мощность присоединения к сетям – 18,6 МВт, и мы не испытываем тех проблем, которые могут возникнуть у объекта, находящегося в пределах МКАД.

Важный момент – транспортная доступность. Даже если ЦОД находится внутри третьего транспортного кольца, то с учетом московского трафика добраться до него не всегда можно быстро. Зеленоград хорош тем, что сюда идут и обычная дорога, и платная, поэтому в случае необходимости можно «долететь» быстрее, чем внутри Москвы.

Сегодня очень актуально создание георазнесенных, катастрофоустойчивых систем. Если основная система находится в Москве, то резервную правильно располагать на удалении, чтобы обеспечить независимость в плане как энергетики, так и связности. Наша площадка в Зеленограде видится едва ли не идеальным местом для размещения такого резерва.

Отмечу и плюсы нахождения в особой экономической зоне. Статус резидента ОЭЗ дает нам существенные экономические преимущества: нулевые таможенные пошлины и нулевой НДС на ввозимое на территорию компании импортное оборудование, пониженную ставку на прибыль, льготы по налогам на фонд оплаты труда, налогу на имущество. Кроме того, мы имеем дополнительную физическую защиту: первый периметр безопасности – самой ОЭЗ, второй – собственно ЦОДа.

– Насколько уход из России почти всех основных зарубежных поставщиков инженерного оборудования затруднил эксплуатацию ЦОДа GreenBushDC? Как компания решала возникшие проблемы?

– Тема острая. Да, сложности с поставками возникли у всех. Мы справляемся с этими вызовами частично импортозамещением, частично – зарубежными аналогами. Для эксплуатируемых систем (ДИБП, ДГУ, система охлаждения и пр.) заключены сервисные контракты, и наши партнеры выполняют все свои обязательства. Они нашли способы поставки запчастей и расходных материалов. Поэтому мы не видим существенных рисков с точки зрения эксплуатации имеющихся систем.

Сегодня мы ориентируемся в основном на российские решения. Планируем установить отечественные системы охлаждения. ИБП также рассматриваем российские. Правда, АКБ, видимо, придется брать китайские – литий-ионные аккумуляторы у нас пока не выпускают.

– Вы ориентируетесь на услуги colocation. Какие тенденции вы видите в области предоставления таких услуг?

– Несмотря на общую тенденцию ухода в облака, colocation продолжает развиваться, у этих услуг есть клиенты. Например, банки, сервисные компании. Да и облач-

ные провайдеры используют услуги colocation для размещения своих платформ.

Из тенденций отмечу рост мощности, потребляемой стойкой. Если пять лет назад стандартом было 5 кВт на стойку, то сейчас мы видим решения на 10, 12, 14 и даже 20 кВт. Вместе с ростом энерговооруженности стойки растут и требования к отводу тепла от нее. Также мы фиксируем тренд к повышению температуры в машзалах, что положительно сказывается на экономике ЦОДов.

Отдельно стоит упомянуть появление у клиентов интереса к стойкам OCP. Сейчас мы как раз тестируем такое решение, проверяем его в разных режимах, в том числе при повышенной температуре. Преимущества OCP – более плотная компоновка ИТ-оборудования, возможность дальнейшего повышения средней температуры в зале, а значит, снижение затрат на охлаждение.

– Какие преимущества дает ЦОДу нахождение в составе группы компаний МТС?

– Во-первых, отмечу доступ к клиентской базе МТС – мы можем предлагать свои услуги более широкому кругу лояльных заказчиков – и к системе закупок МТС. Увеличение масштаба закупок дает существенную экономию при приобретении оборудования.

Во-вторых, доступ ко всей магистральной сети МТС. А это десятки тысяч километров оптики и точки обмена трафиком по всей России. Благодаря надежности и развитости коммуникаций мы можем предоставлять нашим клиентам отличные по качеству и составу услуги связи.

В-третьих, мы пользуемся всеми наработками МТС в области строительства ЦОДов. Компания активно развивает направление модульных ЦОДов, edge-ЦОДов, в том числе в регионах. В них обкатываются новые технологические решения. И эти наработки будут использованы в новых модулях GreenBushDC.

– Ну и традиционный вопрос о планах развития.

– На текущий момент в коммерческой эксплуатации находится один модуль (A2) общей мощностью 6 МВт (ИТ-мощность – 3 МВт). В планах на 2023–2024 гг. – строительство модулей A1 и A3. После ввода их в эксплуатацию мощность ИТ-нагрузки нашего ЦОДа достигнет 9 МВт. Хотя для новых модулей выбраны другие технические решения, они будут не хуже, а скорее, лучше модуля A2. ЦОД станет еще более привлекательным для клиентов.

Как ЦОД, входящий в группу компаний МТС, мы планируем развернуть кластер МТС Cloud для предоставления нашим клиентам комбинированных услуг: вместе с colocation они смогут на той же площадке оперативно получить и облачные ресурсы. Это особенно удобно, когда требуется быстрое увеличение вычислительной мощности или ресурсов хранения. Облачный кластер собираемся запустить в эксплуатацию уже в этом квартале. Как реализуем планы и что уже сделано, приходите и посмотрите сами. С удовольствием проведем вам экскурсию. Заявку можно оставить на сайте cloud.mts.ru/services/colocation-gbdc.



СКС для ЦОДов

Поддержка высоких скоростей передачи данных, высокая плотность и удобство эксплуатации – вот, пожалуй, ключевые характеристики кабельных систем для современных дата-центров.

Стремительный рост объема генерируемых данных продолжается, и основную нагрузку по их приему, обработке и хранению несут ЦОДы. У самих дата-центров «кровеносной системой», по которой передаются гигантские объемы данных, является СКС. Она должна быть не только высокопроизводительной «в моменте», но и обеспечивать в будущем переход на все более высокие скорости, которые способны поддерживать активное сетевое оборудование.

Жажда скорости

На магистраль современных ЦОДов типичными уже стали скорости 200 и 400 Гбит/с, а гиперскейлеры строят сети с перспективой поддержки 800 Гбит/с. Понятно, что такие скорости может обеспечить только оптоволокну. «Медь» остается, но лишь как инфраструктурное решение для мониторинга и обслуживающих систем.

Существуют два основных способа повышения производительности оптической сети. Первый – параллельная передача трафика по нескольким волокнам, или параллельная оптика. Сегодня это основной, наиболее распространенный способ. В качестве «рабочей лошади» в ЦОДах (на расстояниях до 150 м) выступает многомодовое волокно класса OM4. В базовом варианте одна пара OM4 передает поток 10G – это проверенные годами, надежные технические решения. Объединением восьми таких волокон получаем канал 40 Гбит/с, а 20 – 100 Гбит/с. Также практикуют передачу по одному волокну потоков 25G и 50G – из них можно «собрать» каналы 100, 200 и 400 Гбит/с.

Второй способ – спектральное уплотнение (WDM), или передача по одному волокну нескольких потоков на разных длинах волн. В случае многомодового для реализации WDM требуется более дорогое волокно класса OM5, а также более сложное и капризное оборудование. Если еще учесть ограничение доступа российских заказчиков к высоким технологиям, то становится понятно, почему этот вариант пока не получил распространения.

Увеличение числа волокон при использовании параллельной оптики в настоящее время не требует каких-либо существенных технологических пространств. На рынке представлены очень компактные кабели, например, в современный 3-мм ленточный кабель уместается 12 волокон. Большую на-

грузку на кабельные лотки такие кабели не создают – раньше, когда волокна шли отдельными парами, места требовалось больше, не говоря уже о тоннах громоздкой меди.

Для подключения серверов, как и для формирования магистралей, сегодня также используют оптику. Активные кабели, одно время очень популярные, уходят в прошлое. Скорости быстро растут, трансиверы устаревают, такие кабели приходится часто менять, поэтому заказчики от них отказываются. Для гиперскейлеров и коммерческих ЦОДов 10 Гбит/с на сервер обычно достаточно, в высоконагруженных корпоративных и облачных ЦОДах могут использоваться 40- и даже 100-Гбит/с подключения серверов.

Архитектура – проще, плотность – больше

Архитектура сетевых инфраструктур ЦОДов развивается по пути упрощения. Проще – значит, надежнее. Оставляют основные узлы и убирают все промежуточное, все, что можно убрать. Поэтому все реже реализуется концепция ToR (Top of the Rack), т.е. размещение коммутаторов в каждой стойке. Например, гиперскейлер получает полностью подготовленную (претерминированную) стойку с серверами. В плане сетевого оборудования она полностью пассивная. В ней имеется только коммутационная панель, от которой по многомодовой оптике идет подключение к центру коммутации.

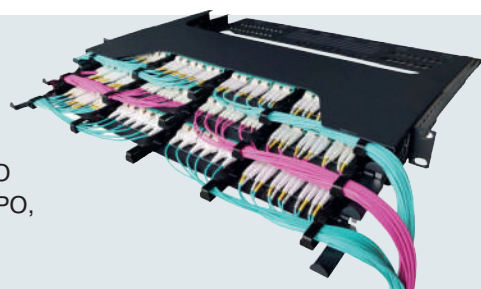
От серверных стоек до центра коммутации в машзале обычно не более 100–120 м. На таком расстоянии отлично работает многомодовая оптика OM4. Далее уже магистральная линия, здесь расстояния больше. Поэтому в крупных ЦОДах на магистрали прокладывают одномодовую оптику.

Технологическое пространство в ЦОДах – ресурс дорогостоящий, и для СКС выделяют минимум места и применяют практически только высокоплотные решения. Средняя плотность составляет 72 дуплексных LC-коннектора (144 волокна) на 1U. При использовании групповых разъемов, например популярных MPO-12, плотность увеличивается в шесть раз. А если взять MPO-24, то в 12 раз, т.е. 1728 волокон на 1U!

Именно групповые соединители MTP/MPO сегодня наиболее популярны в ЦОДах. Но у них есть один серьезный недостаток – высокие потери на соединениях. Для их снижения применяют коннекторы с высококачественными ферулами Low Loss, а это увеличивает стоимость коннекторов

Преимущества СКС DATALAN для ИТ-инфраструктуры зданий и ЦОДов

- Возможность гибкого конфигурирования в соответствии с поставленными задачами
- Высокая степень локализации производства кабельной продукции в РФ
- Соответствие стандартам ISO/IEC 11801, сертификация РФ, TP TC 004, ISO
- Собственное производство: оптические сборки и патч-корды, включая MPO, радиочастотные сборки, производство сертифицировано Huber+Suhner
- Системная гарантия 25 лет





DATALAN на рынке СКК

Борис Грановский,
руководитель направления ЦОД ООО «СКК»
(Группа компаний НКТ)

О ситуации и объеме рынка СКК

После ухода основных западных вендоров освободившиеся ниши пытаются занять многие российские производители. А времени для этого не слишком много, поскольку, считаю, через два-три года зарубежные компании вернуться. Надо успеть укрепить и захватить рынок.

По нашим подсчетам, объем рынка оптических СКК составляет около 200 тыс. коннекторов в месяц. Столько потребляют все заказчики, включая ЦОДы. Мы рассчитываем нарастить наши производственные мощности до уровня 20–30 тыс. коннекторов в месяц, т.е. речь идет о 10–15% рынка оптических СКК.

Об СКК-решениях DATALAN

Мы примерно на 85–90% обеспечиваем функционал, который предлагали западные вендоры, причем по ряду показателей наши решения лучше. Оставшиеся 10–15% – это оптические шкафы высокой плотности. Западные изделия при глубине 200–300 мм поддерживают до 20 тыс. портов. Наши шкафы пока имеют более скромные показатели, но уже в этом году планируем выпустить новое решение, которое будет иметь те же характеристики, что и лучшие зарубежные продукты.

DATALAN использует комплектующие ведущих мировых производителей и лучших заводов в РФ. Так, вся кабельная продукция, кроме ленточных оптических кабелей, производится в России по нашим техническим заданиям. Все коннекторы – импортные. Оптические коннекторы в основном от компании Senko, но используем продукцию и других производителей. Сейчас расширяем собственную площадку по производству медных и оптических сборок.

У нас небольшая команда, мы быстро реагируем на специфические требования заказчиков. Даже если продукт нужно сильно доработать, на это уйдет не более трех месяцев. А, скажем, просто заменить коннекторы MPO-8 на MPO-12 сможем за несколько дней.

О важных особенностях

Мы исторически все делаем из металла (панели, организаторы и пр.), направляющие – на подшипниках. Это проще и надежнее, заказчикам нравится. Пластик, на который перешли почти все другие производители, конечно, легче, но он ненадежен – со временем крошится и ломается.

Еще одно принципиальное отличие от других российских производителей заключается в том, что каждый кабель мы снабжаем сертификатом проверки с указанием реально измеренных характеристик. Для ЦОДов это важно. Есть в нашей продукции и масса приятных мелочей. Например, на панели высокой плотности можно на одном лезвии комбинировать кассеты MPO-8 и MPO-12, это мало кто умеет. Кассеты у нас выдвигают как вперед, так и назад, что удобно при эксплуатации.

и усложняет обслуживание. Перспективными выглядят новые коннекторы CS/SN. Принцип физического контакта в коннекторах CS/SN обеспечивает меньшие потери, чем в MTP/MPO-коннекторах, компактный формфактор позволяет в несколько раз увеличить плотность инсталляции по сравнению с традиционными LC: вместо одного дуплексного коннектора LC можно установить три дуплексных SN. Более того, четыре дуплексных SN-коннектора можно соединить в единый блок, т.е. получить соединитель на восемь волокон. Однако пока техника CS/SN не получила массового распространения.

Инсталляция и эксплуатация

Простые и понятные процедуры эксплуатации с защитой от ошибок, связанных с человеческим фактором, – важное условие надежной работы любой технической системы, включая СКК. В современных условиях также повышается значимость оперативного выполнения различных процедур. Это и сокращение времени монтажа, и возможность быстрого внесения изменений в инфраструктуру. Для этого необходима типизация (стандартизация) решений – изобретать различные варианты подключения для каждой стойки не стоит.

Существенно сократить время монтажа и внесения изменений помогают претерминированные кабельные сборки, которые в основном и используются в ЦОДах. Применение таких сборок также позволяет гарантировать качество соединений. Сегодня уже почти никто не терминирует и не сваривает оптику на площадке – на производстве это сделать проще, причем качество будет выше, а характеристики более повторяемыми. Определенный запас претерминированных сборок на объекте позволит минимизировать время восстановления.

Для надежного функционирования инфраструктуры важно постоянно отслеживать состояние кабельных соединений. Для этого еще на этапе проектирования надо создать, а потом тщательно вести кабельный журнал. Как показывает опыт, в большинстве случаев специалисты продолжают использовать «старые добрые» таблички Excel. Это простой и достаточно удобный инструмент. Конечно, есть электронные кабельные журналы, есть интеллектуальные системы, позволяющие автоматически фиксировать все отключения/подключения. Но их применение серьезно удорожает проект и далеко не везде оправдано. Скажем, гиперскейлерам, у которых за все время эксплуатации в серверной стойке почти ничего не меняется, такие интеллектуальные СКК точно не нужны.

Говоря о человеческом факторе, нельзя забывать об извечной проблеме отрасли – дефиците квалифицированных кадров. Снижение квалификации обслуживающего персонала требует более надежных решений на этапе проектирования. Оптические решения должны быть максимально крепкими и надежными, чтобы ничего нельзя было обломать нечаянно. Поэтому металлические конструкции предпочтительнее пластиковых.



Космос as a Service

Николай
Носов

Коммерческие ЦОДы все активнее осваивают космос, а гиперскейлеры – предлагают их услуги по сервисной модели. В России планируют наращивать спутниковую группировку и в ближайшей перспективе начать с ее помощью предоставление услуг IoT.

Вычисления на орбите

Человечество все активнее использует космическое пространство, число спутников приближается к 5 тыс. Они служат для навигации и организации связи, проведения финансовых транзакций, наблюдения за космическими объектами, погодой и поверхностью Земли. Пользователи космических сервисов контролируют леса и поля, отслеживают перемещения морских судов и помогают при спасательных работах. Объем собираемых спутниками данных стремительно растет. Для их обработки нужны ЦОДы, и размещать эти ЦОДы целесообразно непосредственно в космосе.

Перспективной выглядит уже отработанная в труднодоступных районах Земли технология периферийных вычислений (Edge Computing). В космических edge-ЦОДах будут обрабатываться первичные данные, а в ЦОДах на Земле – анализироваться агрегированная информация и осуществляться управление. Предварительная обработка на месте повысит оперативность принимаемых решений и снизит нагрузку на каналы связи с облаком в головном ЦОДе.

Космос из облака

Клиентам удобно получать космические сервисы из облака привычного гиперскейлера, и работы в этом направлении уже ведутся: облачные провайдеры налаживают взаимодействие с компаниями, запускающими спутники. Начавшееся в 2020 г. сотрудничество Capella Space с AWS привело к появлению у подразделения

AWS Aerospace & Satellite Solutions облачного сервиса управления спутниковой связью на базе AWS Ground Station (рис. 1, 2). Используя облачный сервис, клиенты могут обрабатывать данные, не беспокоясь о создании собственной наземной станции и управлении ее инфраструктурой. А в каталог открытых данных AWS вошли наборы изображений от спутниковых группировок Sentinel-2, Landsat и GOES.

Партнерство с Google Cloud помогает компании Илона Маска SpaceX обрабатывать данные с низкоорбитальных спутников Starlink. SpaceX активно работает над технологией межспутниковых каналов связи, что в перспективе может привести к выделению отдельных спутников для выполнения вычислений на орбите и построению орбитальной распределенной вычислительной сети.

Спутниковый оператор SES объявил, что Microsoft станет первым облачным провайдером работающей на средней околоземной орбите группировки O3b mPOWER. В рамках глобальной инициативы Azure Space компания Microsoft вместе со SpaceX, спутниковым оператором SES, компаниями KSAT, Viasat и US ElectroDynamics разрабатывает решения, связывающие космические и наземные объекты, в том числе дата-центры. Использование облака MS Azure позволяет хранить и анализировать огромные объемы данных для контроля орбит коммерческих спутников и наблюдения за космическим мусором.

В сентябре 2022 г. SES и Microsoft заявили о расширении партнерства в рамках программы виртуализации спутниковой связи, включающей все

узлы экосистемы – от программно определяемых радиостанций и терминалов до виртуализированных сетей и периферийных вычислений.

Программно определяемое все

В первых спутниках ПО создавалось для специализированного серверного оборудования космических объектов. Использование стандартного серверного оборудования позволяет применять обычное коммерческое ПО, в том числе средства виртуализации и облачные платформы, перейти к программно определяемым гиперконвергентным системам, дающим возможность разным компаниям совместно использовать орбитальные вычислительные ресурсы и программно перепрофилировать спутники для своих задач. В частности, они могут создавать edge-облачка для совместной эксплуатации спутника несколькими пользователями, например, для обработки данных спутниковой съемки или мониторинга распределенных датчиков для приложений интернета вещей.

Уже появились стартапы, занимающиеся созданием спутниковых микроЦОДов. В 2019 г. калифорнийская компания Vector анонсировала планы запуска программно определяемого спутника GSky-1. Цель проекта, выполняемого совместно с Университетом Южной Калифорнии (USC), – развертывание на микроспутниках облачной платформы GalacticSky и предоставление пользователям космических вычислительных мощностей по сервисной модели. Легкая ракета-носитель Vector должна была вывести на орбиту созвездие соединенных между собой каналами связи микроспутников, представлявших собою помещенные в прочные контейнеры микроЦОДы (до 16 виртуальных машин в каждом). Такой микроспутник-контейнер может кувыряться, терять связь с Землей, ломаться, но работоспособность одного контейнерного ЦОДа не скажется на работе системы в

целом. На основе кластера микроспутников с одинаковыми орбитами предполагалось развернуть облачную платформу GalacticSky.

Запланированный на конец 2019 г. запуск не состоялся. Но усилия не пропали даром – Lockheed Martin приобрела обанкротившуюся компанию Vector, продолжила сотрудничество с USC и в январе 2022 г. все же запустила GSky-1, правда, под названием Dodona. Компания позиционирует его как первый спутник, использующий программно определяемую спутниковую архитектуру SmartSat. Система работает на платформе NVIDIA Jetson и включает решение для создания приложений искусственного интеллекта NVIDIA JetPack. Системы ИИ задействуются для обработки изображений и цифровых сигналов.

В мае 2021 г. стартап из Сан-Франциско Loft Orbital в рамках программы инновационных исследований для малого бизнеса получил контракт с Космическими силами США для разработки edge-компьютера, который способен анализировать данные в космосе. Loft Orbital предлагает заказчикам размещать полезную нагрузку на борту своих спутников и управлять ею через веб-портал Cockpit, а также планирует самостоятельно разрабатывать космические сервисы, которые будут предоставляться со спутника по модели SaaS.

Базирующаяся во Флориде компания OrbitsEdge предлагает использовать на орбите модель colocation, монтируя серверы в стандартную 19-дюймовую серверную стойку с объемом для оборудования 5U и подключая их к защищенной от неблагоприятного воздействия космоса запатентованной компанией шине OrbitsEdge SatFrame Constellation. По сути, стандартные серверы будут размещаться в космическом микроЦОДе (рис. 3).

На борту первых двух спутников SatFrame будут установлены серверы HPE EL8000. В планах

Рис. 1. AWS Ground Station обеспечивает взаимодействие клиентов со спутниками ◀

Рис. 2. Спутник Capella Space ▼



Основные преимущества космических ЦОДов

- Повышение оперативности обработки информации вплоть до обработки в режиме реального времени.
- Снижение нагрузки на дорогие и имеющие низкую пропускную способность каналы связи с Землей.

Источник: AWS

Источник: Capella Space



Рис. 3.▲
Компонентный состав космического микроЦОДа SatFrame

Источник: laptrinhx.com

Рис. 4.▶
МКС. Светлые квадраты – излучающие радиаторы

Источник: «Роскосмос»

компании – начать с низкой околоземной орбиты, затем перейти на геосинхронную околоземную орбиту и окололунные локации. В январе 2022 г. OrbitsEdge подписала договор о намерениях с компанией Rogue Space Systems, которая в течение 10 лет будет предоставлять для микроЦОДа услуги транспортировки, заправки, орбитальной инспекции (периодической присылки роботизированного корабля) и технического обслуживания. Для обслуживающих космический микроЦОД роботов не нужна дорогостоящая среда, необходимая для работы человека.

Технологические проблемы

В любой ЦОД должна поступать энергия, а потом с вычислительного оборудования должно отводиться выделяющееся тепло. Для дата-центров имеет смысл использовать возобновляемые источники энергии, в частности солнечные батареи. В американских космических кораблях часто применяли химические источники, например, в «Аполлонах» – водородно-кислотные. Но для долго находящегося на орбите дата-центров такой подход вряд ли целесообразен, особенно если учесть, что химическая реакция идет со значительным выделением тепла, а отвод тепла в космосе – сложная задача.

Для традиционного охлаждения космос не пригоден: вакуум – отличный теплоизолятор. Чтобы осознать это, достаточно вспомнить вакуумные колбы в бытовых термосах. Космос пустой, для классического (на основе теплопроводности и конвекции) охлаждения в нем слишком мало частиц, даже с низкой энергией. И чем дальше от поверхности планеты, тем их меньше. В глубоком космосе единственный способ передачи тепла – излучение.

На космических аппаратах (КА) для передачи тепла окружающей среде используются специальные радиаторы, излучающие в ИК-диапазоне. Они могут быть пассивными, когда излучаемое тепло передается им благодаря теплопроводности узлов крепления, или активными, с прокачиваемым через них теплоносителем. На МКС в качестве теплоносителя внешнего контура используется аммиак, внутреннего – обычная вода. Радиаторы (светлые секции на рис. 4 – чем цвет поверхности ближе к белому, тем она сильнее излучает и меньше поглощает тепло) позволяют станции отдавать в окружающее пространство всего 70 кВт тепловой мощности, при этом по размерам они больше жилых модулей станции. И их площадь сравнима с площадью солнечных батарей (темные секции).

Даже для небольшого по современным меркам ЦОДа на 200 стоек площадь поверхности подобных радиаторов должна быть почти в 20 раз больше. Окупаемость такого космического монстра трудно себе представить, а ведь еще значительно возрастут риски столкновений с другими объектами на орбите. Так что по крайней мере ближайшее будущее – только за микроЦОдами.

Для мощных КА придется искать другие пути охлаждения. Согласно закону Стефана – Больцмана, полная испускательная способность абсолютно черного тела пропорциональна четвертой степени его температуры. Поэтому для охлаждения космических ЦОДов будущего, скорее всего, придется разрабатывать сильно раскаляющиеся высокотемпературные радиаторы. При этом они должны по минимуму получать энергию извне. Главный источник энергии на орбите – Солнце, так что отводящие тепло излучатели-радиаторы надо держать либо параллельно солнечному свету, либо в тени.

При создании КА требуется учитывать обмен энергией не только аппарата и космических тел, но и всех приборов и устройств, а также ориентацию спутников относительно источни-

Направления развития космических коммерческих ЦОДов

▶ Взаимодействие, вплоть до организации отдельных каналов связи, облачных провайдеров с запускающими вычислительную нагрузку в космос компаниями. Предоставление космических сервисов из привычных клиентам облаков гиперскейлеров.

▶ Снижение стоимости космических микроЦОДов, в том числе за счет применения стандартного коммерческого вычислительного оборудования.

▶ Снижение стоимости космических сервисов за счет совместного использования ресурсов и программно определяемой архитектуры.

ков как прямого, так и отраженного от других объектов излучения. Для того чтобы одно оборудование не перегревалось другое, третье не замерзло и чтобы на борту КА поддерживалась рабочая температура, разрабатывается отдельная служебная система обеспечения теплового режима. Чем больше вычислительной нагрузки на борту, тем больше надо отводить энергии и тем сложнее обеспечивать тепловой режим.

В зависимости от типа орбиты температура внешней оболочки может меняться от -170° до $+120^{\circ}$. Солнечные батареи не всегда могут вырабатывать электричество, поэтому нужны достаточно емкие накопители энергии для обеспечения работоспособности системы в тени.

Спутники работают в условиях жесткого излучения. Вспышки на Солнце могут выводить из строя электронику, нарушать работоспособность каналов связи с другими спутниками и с Землей. И не стоит забывать о безопасности. Специфическая угроза – столкновение с другими космическими объектами на орбите, прежде всего с космическим мусором. Окружение ЦОДа следует контролировать и при необходимости корректировать орбиту.

Впрочем, для небольших бортовых дата-центров проблемы решаемые, что показал эксперимент с размещением обычных коммерческих серверов на МКС. В феврале 2021 г. Hewlett Packard Enterprise в партнерстве с NASA развернула на Международной космической станции edge-ЦОД с доступом через облако Microsoft Azure. Spaceborne Computer 2 представляет собой ящик с контейнерами, в каждом из которых установлен сервер HPE Proliant DL360 Gen10 для высокопроизводительных вычислений и оснащенная графическим процессором конвергентная edge-система Edgeline EL4000. Работа вычислительного комплекса была признана удовлетворительной, но все же этот edge-ЦОД работал в относительно комфортной среде МКС, пригодной для жизни человека. На безлюдных спутниках вычислительная нагрузка должна работать в более жестких условиях.

Взгляд в будущее

Разработчики дата-центров смотрят дальше орбиты и уже планируют разместить их на других космических объектах. Для начала – на Луне. Принимавшая участие в работах на МКС американская компания Lonestar Data Holdings в апреле 2022 г. объявила о создании серии ЦОДов на лунной поверхности. Компания заключила контракт на первых два полета на Луну и сборку на ней первого дата-центра. Lonestar занимается разработкой сервера, а за проект спускаемого аппарата Nova-C и его посадку отвечает компания Intuitive Machines.

Технологические проблемы космических ЦОДов

- Сложность отвода тепла. Отводить можно только излучением, что трудно реализовать при большой мощности.
- Сложность расчетов ориентации ЦОДа относительно источников прямого и отраженного излучения и поддержания рабочей температуры на борту космического аппарата.
- Риски столкновения с другими космическими объектами и космическим мусором.
- Необходимость защиты вычислительного оборудования от вспышек на Солнце и радиационного воздействия.

Пилотный «лунный ЦОД» предполагается доставить на поверхность нашего спутника до конца 2024 г. и разместить вблизи холмов Мариус в океане Процелларум в вырытой роботами шахте. Активного обмена данными с Землей на первом этапе не планируется – микроЦОД, скорее, будет играть роль резервного бэкапа с самой важной и неизменяемой информацией планеты. Непонятно правда, кто сможет ею воспользоваться, если на Земле произойдет какой-либо глобальный катаклизм, когда этот бэкап понадобится. В случае успешного завершения работ в дальнейшем будет налажен полноценный обмен информацией между Землей и Луной.

Планы России

По количеству спутников в космосе Россия отстает от лидирующих США и Китая, и отставание увеличивается. Если в 2011 г. доля российских спутников в мировой группировке составляла 8%, то в начале 2021 г., по данным USC, снизилась до 4%. За это время количество спутников у России удвоилось и достигло 169, но у лидеров рост семикратный: у США до 2944, у Китая до 499. Нас обогнала и показавшая рост в 25% Великобритания (452). Рывок США обеспечен во многом за счет 1815 мини-спутников связи Starlink, успехи британцев – 394 аппаратами OneWeb. За первую половину 2022 г. Россия совершила еще 10 запусков, что добавило 16 спутников, но отставание от лидеров все равно велико.

Отрыв помогут сократить запуски спутников в рамках проекта национальной многофункциональной инфокоммуникационной спутниковой сети «Сфера» (рис. 5), российского ответа Starlink и OneWeb. В октябре 2021 г. тогдашний глава «Роскосмоса» Дмитрий Рогозин на 72-м Международном астронавтическом конгрессе в Дубае сообщил, что по программе «Сфера» принято решение сформировать пять группировок связи (спутники серии «Ямал», «Экспресс-РВ», «Экспресс», «Скиф», «Марафон IoT») и пять группировок наблюдения в различных диапазонах («Смотр», «Беркут-О», «Беркут-S», «Беркут-VD», «Беркут-X, L, P»).



Рис. 5. ▲ Многофункциональная спутниковая телекоммуникационная инфраструктура, создаваемая в рамках программы «Сфера»

Источник: Ассоциация участников рынка спутниковой связи

В 2022–2030 гг. предполагается запустить на орбиты до 156 новых спутников гражданского назначения для глобальной связи, вещания, ШПД и IoT. В результате к 2030 г. общая информационная емкость российской спутниковой инфраструктуры связи и вещания составит 274 Гбит/с. Эта инфраструктура должна обеспечить решение всех перспективных задач РФ до 2045–2050 гг.

В январе 2022 г. стало известно о выделении государственного финансирования для спутникового проекта «Марафон IoT». Предполагается, что в состав группировки «Марафон IoT» войдут 264 аппарата, которые будут размещаться в 12 орбитальных плоскостях на высоте около 750 км. Проект и техническое задание на разработку эскизного проекта представила компания «Информационные спутниковые системы им. акад. М.Ф. Решетнёва». Первый спутник в рамках этого проекта намечено запустить в 2024 г. К 2025 г. планируется начать создание глобально распределенной спутниковой сети IoT, интегрированной с наземными сетями, а также предоставление типовых сервисов IoT на основе бесшовности с наземными сетями.

Помимо «Марафон IoT» в программу «Сфера» входит проект «Скиф», в рамках которого преду-

сматривается запуск 12 спутников для широкополосного доступа в интернет. Причем первый спутник по программе «Сфера» уже работает: 23 октября 2022 г. на орбиту выведен спутник «Скиф-Д», предназначенный для отработки технических решений и защиты орбитально-частотного ресурса будущей группировки «Скиф».

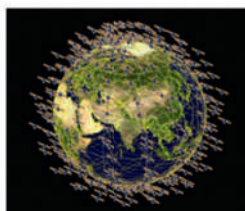
На конференции Satcomrus-2022 председатель совета Ассоциации участников рынка спутниковой связи Юрий Урличич рассказал о планах создания конкурирующей с «Марафон IoT» группировки Telum-Leo-1 (рис. 6), которая также будет работать в рамках концепции интернета вещей, но с другими параметрами. В новую группировку войдут 144 основных космических наноаппарата и восемь резервных. Ширина грани наноКА 10 см, высота 3,4 см, масса 1,5 кг, мощность солнечной батареи 8 Вт.

«К 2025 г. планируем предоставление специальных сервисов IoT, требующих работы в реальном времени, для беспилотных систем», – сообщил Ю. Урличич. По его словам, ассоциация ожидает, что к 2035 г. рынок будет насчитывать 10 млн офлайн-пользователей интернета вещей, 1 млн онлайн-пользователей и 30 млн тех, кто получит доступ к «Кнопке жизни».

Запуск низкоорбитальных спутников – наиболее дешевое и массовое решение, позволяющее устройствам без дорогостоящего наземного оборудования работать непосредственно со спутником. С учетом режима санкций вряд ли будет возможным использовать зарубежные спутниковые группировки для российских проектов, поэтому надо создавать свои, в том числе с edge-ЦОДами на борту. И конечно, разрабатывать российские облачные решения для управления коммерческими спутниковыми проектами, создавать свой Космос as a Service. ИКС

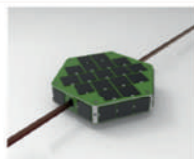
Рис. 6. ▼ Telum-LEO-1: группировка передачи данных на базе наноКА

Орбитальное построение
8 орбитальных плоскостей
18+1 наноКА в плоскости (144+8)
Наклонение: 98°
Начальная высота круговой орбиты: 585 км
Конечная высота круговой орбиты: 385 км
CAC: 3 года



Планируемая дата запуска экспериментальных наноКА TELUM-LEO-1E (2 наноКА): декабрь 2023 г.

Параметры наноКА
Ширина грани: 10 см
Высота грани: 3,4 см
Масса: 1,5 кг
Мощность солнечной батареи: 8 Вт

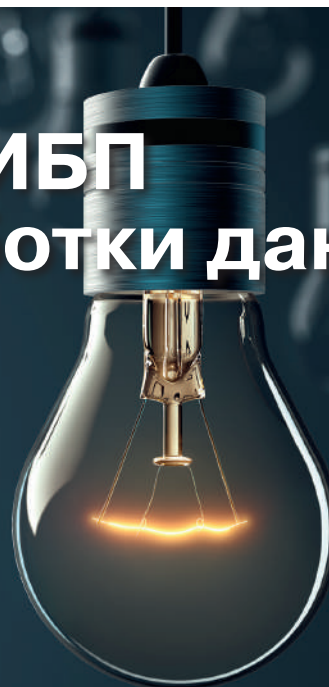


Радиочастотное обеспечение
Решение ГКРЧ от 28.03.2022 №22-62-02-01
Заявка в МСЭ от 20.06.2022 ID 122520078
Тх: 137-138 МГц; 400,15-401 МГц
Рх: 149,95-150,05 МГц; 399,9-400,05 МГц

Источник: Ассоциация участников рынка спутниковой связи

Критерии выбора ИБП для центров обработки данных

Самый страшный сон инженера дата-центра – это конец света, только не солнечного, а электрического. Поэтому к выбору ИБП при создании ЦОДа нужно подходить основательно.



При отключении основного источника электроэнергии именно ИБП будут поддерживать электропитание критической нагрузки до безопасного завершения рабочих процессов или включения резервной ДГУ. В нормальном режиме работы это оборудование тоже не стоит без дела: оно защищает критическое ИТ-оборудование от негативных факторов, связанных со снижением качества электроэнергии, будь то отклонения от номинала напряжения или частоты, высокочастотные помехи от электромагнитных полей или искажение формы напряжения из-за нелинейных нагрузок.

В этой статье я опишу несколько критериев, которыми руководствуюсь при проектировании систем бесперебойного электроснабжения для дата-центров, а в качестве иллюстрации приведу примеры оборудования тайваньской компании Delta и китайской Kehua Tech. Мой выбор пал на этих вендоров не случайно: во-первых, их продукция доступна на нашем рынке, а во-вторых, в отличие от «российских» производителей, которые в лучшем случае занимают крупноузловую сборку ИБП из готовых компонентов, эти компании имеют собственные производства с несколькими площадками и научно-исследовательскими центрами, многолетний опыт и хорошую репутацию.

Аккумулятор или маховик?

По технологии резервирования ИБП делятся на статические и динамические. В статических ИБП функцию аккумулятирования энергии выполняют устройства, не имеющие вращающихся частей. Это, например, аккумулятор-

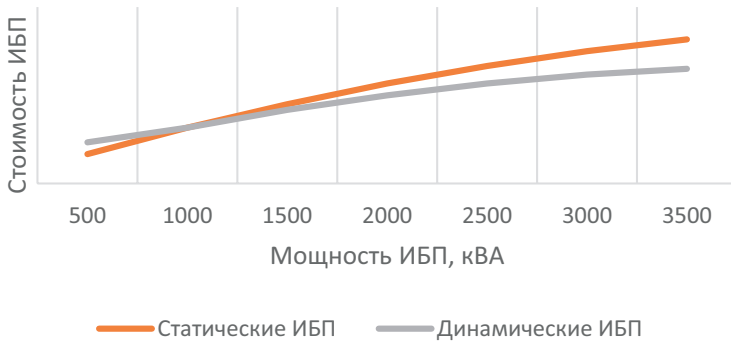
ные батареи, накапливающие и отдающие электрическую энергию за счет протекающих в них химических реакций, или суперконденсаторы (ионисторы), работающие на энергии электрического заряда.

В динамических ИБП кинетическая энергия накапливается с помощью маховика, постоянно вращающегося на одном валу с обратимой (т.е. в зависимости от режима работы выполняющей роль электродвигателя или генератора) электрической машиной. При отключении основного источника электроснабжения маховик отдает накопленную энергию, преобразуемую электрической машиной в электрическую. Это дает время для запуска дизельного генератора, обеспечивая бесперебойное электроснабжение критической нагрузки. Таким образом, дизель-роторные ИБП (ДРИБП) имеют в своем составе маховик, электрическую машину и ДГУ.

Если исходить из капитальных затрат, то при мощности ЦОДа примерно до 1 МВт динамические ИБП не будут иметь преимуществ перед комплексом статических ИБП + ДГУ. Повышение мощности потребует для статических ИБП большего массива аккумуляторных батарей: их количество будет расти пропорционально мощности, а значит, увеличится и цена. Стоимость ДРИБП в аналогичных условиях тоже будет расти, но не так быстро (рис. 1).

Казалось бы, для крупных ЦОДов ДРИБП намного выгоднее. Однако мы не учли затраты на эксплуатацию: аккумуляторные батареи требуют замены в среднем раз в семь лет, в то время как динамическим ИБП необходимо дорогостоящее периодическое обслуживание – постоянно

Игорь Денисов, руководитель группы проектирования систем электро-снабжения, Step Logic



▲ Рис. 1.
Зависимость стоимости ИБП от их мощности

вращающиеся механические части нуждаются в диагностике, смазке, замене подшипников.

При низком уровне нагрузки в ЦОДе эффективность ДРИБП будет снижаться, потери составят большую часть в сравнении с полезной нагрузкой. В то же время статические ИБП модульного типа могут сохранять высокий КПД при разных уровнях нагрузки за счет программного отключения отдельных силовых модулей.

Еще один важный фактор, говорящий не в пользу динамических ИБП, — они обеспечивают автономную работу от маховика не более 30 с. За это время дизель-генератор может не успеть запуститься, поэтому есть риск полного отключения электроснабжения критической нагрузки. Статические ИБП двойного преобразования переходят на работу от батарей мгновенно и дают ДГУ больше времени на запуск (10–20 мин).

И динамические, и статические ИБП довольно капризны и требуют определенных условий для размещения. Для статических ИБП в ЦОДе нужно предусмотреть большие площади под аккумуляторные батареи, а также систему кондиционирования для обеспечения нормативного срока их службы. ДРИБП занимает меньше места (а значит, мы получаем больше площади для полезной ИТ-нагрузки), но для них необходимы приток воздуха, отвод отработанных газов и доступ для обслуживания. Наличие в динамических ИБП системы хранения и подачи топлива также накладывает определенные ограничения.

Существуют решения, объединяющие в себе преимущества как статических, так и динамических ИБП. То есть система бесперебойного электроснабжения работает по принципу ста-

тических ИБП с двойным преобразованием, но вместо аккумуляторных батарей используется динамический модуль с постоянно вращающимся маховиком, кинетическая энергия которого преобразуется в электрическую при отключении основного источника электроснабжения. Поэтому не требуются большие площади для размещения аккумуляторных батарей и обеспечивается двойное преобразование по напряжению и частоте. Однако и основные недостатки, связанные с наличием в системе постоянного вращающегося маховика и небольшим временем автономии, сохраняются.

Таким образом, для ЦОДа мощностью менее 1 МВт предпочтительнее статические ИБП. К ним относятся, например, модели KR33 300–1000 кВА, MR33 400–1000 кВА из линейки Kehua Tech, а также Ultron серии DPS 300–1000 кВА и Modulon серии DPH 300–600 кВт из линейки Delta. Системы бесперебойного электроснабжения с кинетическим накопителем энергии мы рассматриваем, как правило, только если в проекте нет необходимых площадей с системой кондиционирования воздуха для аккумуляторных батарей. При этом нужно сравнить капитальные и эксплуатационные затраты нескольких альтернативных вариантов. Обычно производители специализируются на выпуске только статических или только динамических ИБП из-за принципиально различающейся технологии резервирования.

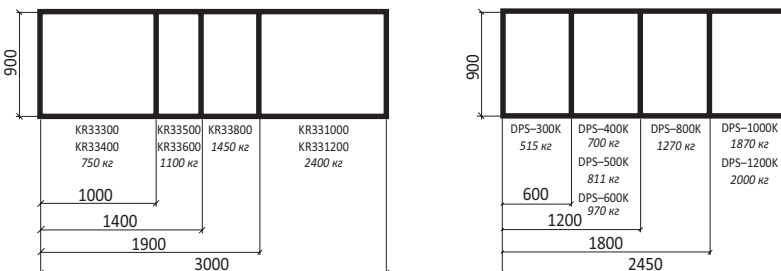
Основные характеристики статических ИБП

Мощность

ИБП делятся на источники малой (до 3 кВА), средней (до 20 кВА) и большой мощности (20–600 кВА и более). Последние применяются для средних и крупных ЦОДов, первые два — для микро- и мини-ЦОДов. При расчете необходимой мощности к максимальной нагрузке ЦОДа обычно добавляют 20–30%. Большой резерв не оправдан из-за больших капитальных затрат и меньшей эффективности, а недостаточная мощность ИБП может привести к перегрузке и отключению защищаемой нагрузки. Кроме того, в зависимости от мощности размеры ИБП значительно различаются: для примера на рис. 2 приведены размеры и веса ИБП Kehua Tech KR33 и Delta DPS разной мощности.

При выборе ИБП необходимо также учитывать коэффициент мощности нагрузки, т.е. проверять соответствие ИБП как полной (измеряемой в ВА), так и активной (измеряемой в Вт) мощности нагрузки. Например, если активная мощность нагрузки равна 9 кВт при коэффициенте мощности 0,8, то полная мощность нагрузки составит 11,25 кВА. Значит, ИБП на 9 кВт с

Рис. 2. Размеры ИБП Kehua Tech KR33 и Delta DPS различной мощности, мм ▼



коэффициентом мощности 0,9 для питания этой нагрузки не подойдет, так как полная мощность ИБП в этом случае равна 10 кВА.

Для определения мощности, потребляемой самим ИБП, обязательно учитываем:

- КПД ИБП;
- необходимость зарядки батарей;
- возможность работы при пониженном входном напряжении (для этого случая необходимо проверить потребляемый ток).

Поскольку ИБП содержит нелинейные полупроводниковые элементы, сопротивление которых зависит от напряжения и тока в их цепи, при подключении его к электрической сети генерируются дополнительные гармонические составляющие тока и напряжения: ток и напряжение на входе ИБП перестают быть строго синусоидальными. Коэффициент мощности PF при этом равен:

$$PF = \frac{P}{S} = \frac{U \times I_1 \times \cos(\varphi_1)}{U \times I}$$

где P – активная мощность, потребляемая ИБП (Вт); S – полная мощность, потребляемая ИБП (ВА); U – действующее значение напряжения на входе ИБП (В); I – действующее значение тока на входе ИБП (А); I_1 – действующее значение первой гармоники тока (А); φ_1 – угол сдвига фаз между напряжением и первой гармоникой тока.

Таким образом, коэффициент мощности PF меньше единицы и определяется не только значением $\cos(\varphi_1)$, но и коэффициентом гармонических искажений тока THD – отношением среднеквадратичного значения всех высших гармоник тока к первой гармонике тока. Поэтому в случаях, когда требуется обеспечить низкий коэффициент THD (не более 3%), ИБП должен иметь схему коррекции коэффициента мощности (PFC) на входе для фильтрации высших гармоник. В технических характеристиках ИБП производители всегда указывают коэффициент мощности PF, а также коэффициент THD.

Топология

ИБП можно разделить на резервные, линейно-интерактивные, с двойным и с дельта-преобразованием. Резервные и линейно-интерактивные ИБП не защищают от всех негативных факторов, связанных со снижением качества электроэнергии основного источника электроснабжения, поэтому для питания критических нагрузок ЦОД они не применяются и в этой статье рассматривать их не будем.

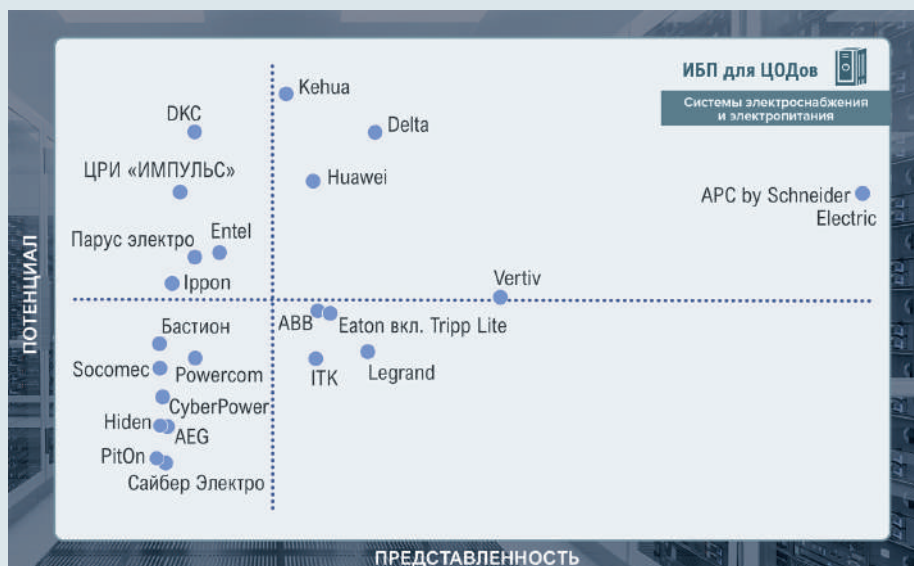
Подробнее остановлюсь на ИБП с двойным и дельта-преобразованием. Принцип работы ИБП первого типа заключается в двойном преобразовании входного тока: сначала входной переменный ток конвертируется в постоянный с помощью выпрямителя, затем в инверторе снова пре-

ИБП: новый ландшафт рынка

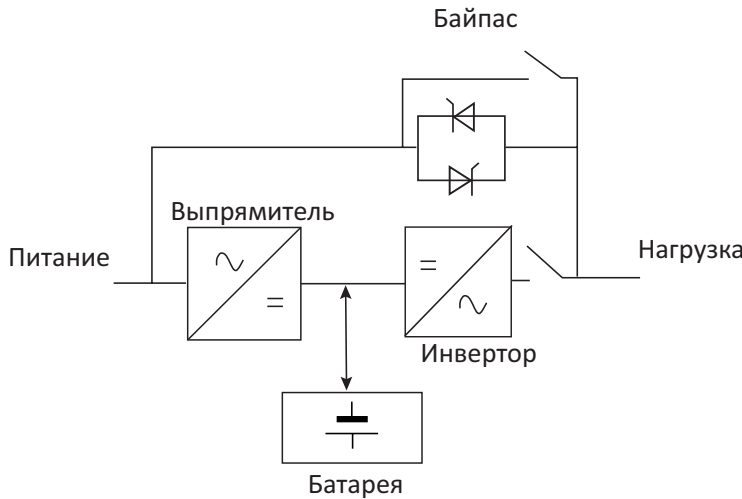
Источники бесперебойного питания – ключевой элемент инфраструктуры дата-центров, обеспечивающий бесперебойное и качественное электропитание ИТ-оборудования. На рынке ИБП для ЦОДов долгое время лидировали западные производители, однако на фоне СВО большинство таких компаний решили уйти из России (или приостановили свою деятельность в нашей стране). Их место активно занимают российские и азиатские производители.

Карта восприятия вендоров в сегменте «ИБП для ЦОДов»

Ситуацию на рынке наглядно иллюстрирует «Карта восприятия вендоров» – исследование, проведенное iKS-Consulting в середине 2022 г. Хотя по показателю «Представленность» (показывает присутствие решений конкретного вендора в инфраструктуре заказчиков) на момент проведения опроса лидировали западные вендоры, наибольшими значениями «Потенциала» (оценка способности вендора к развитию в РФ) обладают российские и азиатские производители.



Источник: iKS-Consulting



▲ Рис. 3. Схема ИБП с двойным преобразованием

образуется в переменный (рис. 3). При этом батареи всегда подключены к схеме, и в нормальном режиме работы поддерживается их заряд, а при аварии в сети нагрузка без каких-либо переключений получает питание от батарей. Таким образом, время на переключение не затрачивается и обеспечивается непрерывность электроснабжения критических нагрузок. Благодаря чистой синусоидальной форме тока на выходе ИБП (регулируется как напряжение, так и частота) к нему можно подключать чувствительную к качеству электроэнергии нагрузку дата-центров: нагруженные серверы, высокопроизводительные рабочие станции локальных вычислительных сетей. Нагрузка полностью защищена от любых электрических помех внешней электросети, высоковольтных импульсов, колебаний входного напряжения и отклонений частоты.

К недостаткам ИБП с двойным преобразованием относятся высокие стоимость (в два-три раза выше, чем стоимость линейно-интерактивных), тепловыделение и уровень шума (из-за наличия вентиляторов, необходимых для отвода тепла). КПД ИБП с двойным преобразованием в онлайн-режиме составляет 80–95%, однако большинство производителей предлагают различные автоматические интеллектуальные

режимы работы, помогающие повысить это значение вплоть до 99%.

Например, в моделях ИБП с двойным преобразованием Kehua Tech MR33 для повышения надежности и эффективности реализованы:

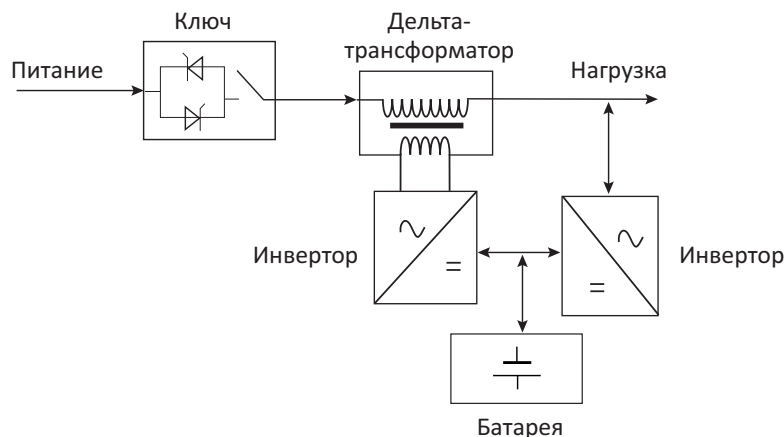
- трехуровневая технология преобразования, благодаря которой улучшается качество выходного напряжения;
- цифровое управление инвертором для контроля синхронизации, выравнивания токов в параллельной системе, управления устройством с высокой точностью и скоростью;
- коррекция входного коэффициента мощности, благодаря чему входной коэффициент мощности ИБП превышает 0,99, что значительно увеличивает коэффициент использования электрической энергии, уменьшает нагрузку на энергосистему и позволяет сэкономить на затратах на электроэнергию;
- экорезим для энергосбережения, в котором ИБП при хорошем качестве входной сети работает на байпасе с КПД, достигающим 99%; когда входное напряжение или частота на входе байпаса не удовлетворяют значениям «разрешенного» диапазона, ИБП переключается на инвертор.

В ИБП Delta серии DPH для того, чтобы обеспечить КПД до 96,5% в онлайн-режиме, а в экономичном режиме – 99%, применяются:

- IGBT-технология (выпрямитель на биполярных транзисторах с изолированным затвором) для обеспечения высококачественного, с низкими помехами, чистого и бесперебойного выходного питания для подключенных нагрузок;
- интеллектуальный экологичный режим работы, который обеспечивает агрегирование мощности всех силовых модулей, позволяя поднять КПД двойного преобразования и уменьшить потери энергии; система автоматически подсчитывает, какой процент текущая нагрузка ИБП составляет от максимально возможной, и на основании этого решает, какие силовые модули включить, а какие оставить в режиме ожидания, чтобы обеспечить максимальный КПД.

ИБП с дельта-преобразованием состоит из двунаправленных инверторов, связанных с общей батареей (рис. 4). При понижении входного напряжения первый из инверторов работает как выпрямитель, а второй – как инвертор. При повышении входного напряжения их роли меняются. Нагрузка связана с сетью через трансформатор с дополнительной обмоткой, на которую подается компенсирующее напряжение от дельта-инвертора, пропорциональное, но противоположное по фазе отклонению входного напряжения. В основном режиме эффективность этих ИБП выше, чем у ИБП двойного преобразования.

Рис. 4. Схема ИБП с дельта-преобразованием ▼



Высокий КПД достигается за счет того, что преобразование электроэнергии происходит только в объеме, необходимом для поддержания заданных параметров напряжения и тока, и переход на работу от батарей переключения не требует. На практике же КПД зачастую снижается из-за недозагрузки ИБП, отклонения параметров входного напряжения от номинальных и нелинейности нагрузки. Так, если при полной нагрузке и высоком качестве входного напряжения у ИБП с дельта-преобразованием КПД равен 96%, то при других условиях он сравним со значениями у ИБП двойного преобразования.

Из минусов таких систем отмечу более сложную схему, которая увеличивает инерционность системы и влияет на стоимость и надежность оборудования. Наличие связи между нагрузкой и сетью не позволяет полностью защитить оборудование от сетевых помех и отклонений частоты. Появляется необходимость в синхронизации инверторов с сетью, а также нескольких ИБП друг с другом при включении их в параллель.

Таким образом, наиболее надежную защиту критической нагрузки обеспечивают ИБП с двойным преобразованием. Неслучайно именно они чаще всего используются в ЦОДах. ИБП с дельта-преобразованием менее распространены: они представлены лишь у небольшого числа производителей, а их преимущества имеют значение при более высоком качестве электроэнергии основного источника.

Количество фаз на входе и выходе

В зависимости от мощности и параметров конкретной линейки оборудования ИБП имеют различные варианты подключения:

- однофазный вход (один или два входа), однофазный выход (1:1);
- трехфазный вход (один или два входа), однофазный выход (3:1);
- трехфазный вход (один или два входа), трехфазный выход (3:3).

ИБП малой мощности имеют возможность подключения только по схеме «однофазный вход, однофазный выход», большой мощности – по схеме «трехфазный вход, трехфазный выход». Самые гибкие – ИБП средней мощности, их можно подключить любым из трех способов (возможности различных линеек оборудования необходимо уточнять у производителя).

Внимание: при схеме подключения ИБП 3:1 и переключении на байпас вся нагрузка оказывается присоединенной только к одной из фаз питающей линии. При проектировании необходимо соответствующим образом выбирать сечение вводного кабеля и параметры аппарата защиты.

Конструктивное исполнение

ИБП можно разделить на моноблочные и модульные.

Модульные ИБП представляют собой унифицированный шкаф, в котором все основные компоненты сконфигурированы в отдельные модули (силовые, батарейные, модули управления, статического байпаса, распределения) и работают взаимосвязанно, что дает им много преимуществ.

Например, мощность ИБП можно увеличить, установив дополнительные силовые модули. Таким образом, на начальном этапе можно установить минимально необходимое количество модулей, а затем, при росте мощности ЦОДа, силовые модули докупить. На уровне модулей можно реализовать схему резервирования N + 1, при которой выход из строя одного из силовых модулей не окажет влияния на работоспособность всей нагрузки.

Любой из модулей можно установить, демонтировать или заменить силами персонала заказчика без отключения ИБП: на электроснабжение критической нагрузки эти действия не окажут никакого влияния. При этом замена не займет много времени.

Модульными ИБП являются, к примеру, Kehua Tech MR33 и Delta DPH-серии. Однако нужно иметь в виду, что реализация модульности компонентов ИБП может различаться от производителя к производителю. Например, у ИБП Delta DPH-серии каждый силовой модуль включает в себя собственный контроллер, в отличие от ИБП Kehua Tech MR33, где модуль управления общий на весь ИБП. Также для ИБП Delta DPH-серии существуют батарейные модули с функцией «горячей» замены, тогда как для Kehua Tech MR33 таких батарейных модулей нет.

Но если необходимости в наращивании мощности нагрузки в будущем нет, не требуется резервирование на уровне силовых модулей или оно выполнено на уровне ИБП, то вполне достаточным может быть применение моноблочных ИБП. Их стоимость на 20–50% ниже, чем модульных. Кроме того, современные моноблочные ИБП часто имеют модульную компоновку основных элементов. Они расположены в одном корпусе, а замена их возможна только силами сервисного персонала. К таким ИБП относятся, например, Delta HPH-серии, Delta DPS-серии, Kehua Tech MY, Kehua Tech KR33.

Необходимо отметить, что как моноблочные, так и модульные ИБП малой и средней мощности можно разместить в ИТ-стойке с помощью комплекта специальных направляющих или установить непосредственно на полку стойки.

Тип поддерживаемых аккумуляторов

Самый распространенный тип аккумуляторов электроэнергии для ИБП – свинцово-кислотные. Технология их производства хорошо изучена, они надежны, выдерживают до 1000 циклов заряда-разряда, имеют небольшой саморазряд, работают в достаточно широком диапазоне температур, у них нет эффекта памяти. Среди недостатков – низкая удельная емкость, следствием чего являются большой вес и размеры. Срок службы также небольшой – в среднем семь лет, он зависит от условий хранения и эксплуатации, количества циклов заряда-разряда, глубины разряда в каждом случае и продолжительности разряженного состояния.

Современные технологии производства свинцово-кислотных батарей – это GEL (электролит имеет структуру геля из-за добавления в него стабилизатора – силикагеля) и AGM (электролит находится в порах специальной стеклоткани, которая расположена между свинцовыми пластинами). Преимущества этих технологий – безопасность в эксплуатации, нечувствительность к положению, низкий саморазряд.

Не все производители ИБП выпускают также и аккумуляторы. У Delta есть свои линейки батарей, широко представленные на рынке: например, к линейке Delta Xpert, разработанной специально для использования в «тяжелых» системах бесперебойного питания ЦОДов относятся и свинцово-кислотные батареи серии HRL-W. Это необслуживаемые АКБ со сроком службы 12 лет, произведенные по AGM-технологии с системой рекомбинации газов (VRLA). Они обладают повышенной токоотдачей благодаря использованию при производстве более толстых электродов, а также высокотехнологичных составов с применением структурных агентов в активной массе.

В последнее время для ЦОДов стали использовать литий-ионные АКБ. Сейчас их стоимость на 20–30% выше, чем свинцово-кислотных, но у них есть ряд неоспоримых преимуществ. Литий-ионные аккумуляторы имеют большую удельную емкость, занимают на 40–60% меньше площади, их вес ниже на 60–70%. Они отличаются меньшим саморазрядом и быстрее заряжаются, а срок их службы достигает 10 и более лет. Таким образом, совокупная стоимость владения за 10 лет эксплуатации получается ниже, чем у свинцово-кислотных.

У Kehua Tech есть линейка ИБП KR-RM Li со встроенными литий-ионными аккумуляторами, а также литий-ионная аккумуляторная система S³ Smart Backup System в формате внешних батарейных шкафов, которая имеет модульную параллельную конструкцию – безопасную, технологичную и простую в использовании. Тип ли-

тий-ионных аккумуляторов – LFP. У Delta также есть батарейные шкафы серии UDL с литий-ионными аккумуляторами по технологии LFP.

Сравнение характеристик свинцово-кислотных и литий-ионных батарей

Характеристики	Литий-ионные АКБ	Свинцово-кислотные АКБ
Энергетическая плотность, кВт·ч/кг	70–260	15–50
Срок службы, лет	10–15	3–5/6–9
Количество циклов заряда/разряда	>3000	200–400
Время полного заряда, ч	0,5–1	6–12
Система мониторинга	Поставляются с системой мониторинга	Чаще всего используются без системы мониторинга
Работа при температурах выше 25°C	Способны работать до 40°C	Срок службы уменьшается

Другие типы аккумуляторов для ИБП центров обработки данных не имеют широкого распространения. У никель-кадмиевых батарей, например, есть эффект памяти, из-за чего они неприменимы для работы с ИБП в режиме кратковременных неполных разрядов. Никель-металлогидридные АКБ имеют высокий уровень саморазряда, небольшую нагрузочную способность, малое количество циклов перезарядки.

Там, где неприменимы традиционные аккумуляторы (например, нет возможности обеспечить помещения системой кондиционирования для поддержания необходимого свинцово-кислотным или литий-ионным АКБ температурного режима), для электроснабжения критической нагрузки на время до 60 с, которое требуется для запуска резервного генератора, можно использовать суперконденсаторы (ионисторы) – электрохимические конденсаторы, отличающиеся от традиционных значительно большей емкостью, удельной мощностью и более низкими токами потерь.

Главный параметр, определяющий емкость конденсатора – активная площадь электродов. В традиционных конденсаторах электроды выполнены из металлических лент, свернутых в цилиндр или скругленный параллелепипед, т.е. увеличение активной площади электрода влечет за собой рост размеров конденсатора. В суперконденсаторах применяются электроды из многостенных углеродных нанотрубок, благодаря чему активная площадь электродов увеличивается до 2000 кв. м на 1 г электрода. Кроме этого, к их преимуществам можно отнести:

- отсутствие необходимости в техническом обслуживании;
- расчетный срок службы до 20 лет;
- диапазон рабочих температур от -40°C до $+65^{\circ}\text{C}$;
- высокую надежность;
- ненужность специальной системы охлаждения, так как при эксплуатации тепло почти не выделяется;
- возможность масштабирования для адаптации к любым мощности и времени автономии;
- малое время зарядки: около 1–2 мин от полностью разряженного состояния;
- малую временную деградацию: суперконденсаторы рассчитаны на 1 млн циклов;
- КПД до 95%;
- малую токсичность материалов, отсутствие движущихся частей и химических реакций.

Суперконденсаторы можно применять, например, вместо динамических ИБП, имеющих сравнимое с ними время резервирования и также не требующих кондиционирования воздуха. При этом необходимо рассчитать капитальные и эксплуатационные затраты при проработке сравниваемых вариантов.

На данный момент не наработан достаточный опыт использования ИБП с суперконденсаторами в качестве аккумуляторов электроэнергии, да и предложение на рынке невелико.

Время автономной работы

Требуемое время автономной работы ИБП в ЦОДе обычно составляет 10–20 мин. Этого вполне достаточно, чтобы запустить резервный источник электроснабжения (ДГУ) или безопасно завершить работу и выключить критическое оборудование. Для того чтобы обеспечить необходимое время автономии, нужно выбирать количество и емкость аккумуляторов в зависимости от величины защищаемой нагрузки.

Однако следует также учитывать, что после отключения сетевого питания и разрядки батарей их необходимо заряжать. Время зарядки тоже немаловажный фактор, особенно в случае большого времени автономии (6–12 ч) при небольшой нагрузке (до 10 кВА). В этом случае для сокращения времени зарядки больших массивов аккумуляторных батарей требуется выбирать ИБП на большую мощность с более мощным зарядным устройством.

Естественно, здесь перечислены далеко не все характеристики, которые стоит принять во внимание при выборе ИБП для ЦОДа. Как минимум еще нужно учесть диапазон входного напряжения, наличие встроенного трансформатора и диспетчеризации, возможность параллельной работы, типы входных и выходных разъемов, перегрузочную способность, массу и габариты оборудования. **ИКС**

23 МАЯ 2023 DATA CENTER DESIGN & ENGINEERING

МОСКВА

Сегодня рынок инженерных систем ЦОДов находится в стадии серьезной трансформации. Вслед за пандемией возникли новые вызовы, связанные с беспрецедентными санкциями. Но 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
- Префабы, модули и контейнерные ЦОДы
- Системы электропитания и охлаждения
- Кабельные системы
- Искусственный интеллект и системы автоматизации
- Наилучшие практики эксплуатации



dcdeforum.ru

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

DCDE
FORUM

10-я КОНФЕРЕНЦИЯ
И ВЫСТАВКА

Новинки от EMILINK: кабеленесущие системы NTSS

Заказчики, обеспокоенные уходом крупных зарубежных производителей пластиковых кабельных каналов, проволочных и перфорированных лотков, могут быть уверены – теперь на рынке есть достойные аналоги, сделанные в России.

2023 г. начался для ГК EMILINK знаменательным событием – запуском производства новой продукции. Российский мультипроизводитель телекоммуникационного оборудования объявил о выводе на рынок кабеленесущих систем под брендом NTSS.

Группа компаний EMILINK более 15 лет на своих производственных площадях выпускает различную телекоммуникационную продукцию. В 2017 г. появилось и собственное производство оптического кабеля. Решение компании изготавливать оборудование для организации кабельных трасс выглядит вполне логичным.

Итак, что предлагает EMILINK?

Кабельные каналы

Пластиковые кабельные каналы (КК) есть в большинстве современных офисов. Они применяются для открытой прокладки электрических и информационных кабелей при организации рабочих мест.

ГК EMILINK предлагает семь типоразмеров кабельных каналов. Это и мини-каналы, и магистральные КК:

- 20 x 12,5 x 2000 мм;
- 40 x 20 x 2000 мм (два вида – со встроенной перегородкой и без нее);
- 60 x 16 x 2000 мм (с двумя встроенными перегородками);
- 75 x 20 x 2000 мм (с двумя встроенными перегородками);
- 100 x 50 x 2000 мм;
- 105 x 50 x 2000 мм;
- 130 x 50 x 2000 мм.

Все поставляемые кабельные каналы имеют съемную крышку.

Широкий ассортимент КК позволяет организовать рабочие места в соответствии с любыми требованиями заказчиков. Кроме самих КК потребителям предлагается большой выбор стандартных комплектующих элементов (аксессуаров). Аксессуары существенно расширяют возможности прокладки и монтажа, а также улучшают эстетические характеристики смонтированных КК.

Для установки на рабочих местах электрических и информационных розеток предусмотрены различные суппорты с рамками, соответствующие принятому в отрасли стандарту «45 x 45». Примененные при их разработке дизайнерские решения обеспечивают эстетичный внешний вид розеток как неотъемлемой части КК. С точки зрения размещения розетки относительно внутреннего пространства КК суппорты делятся на три группы:

- розетки устанавливаются внутрь КК;
- розетки устанавливаются на КК;
- розетки устанавливаются рядом с КК.

Первый способ пригоден для КК 100 x 50 мм, 105 x 50 мм и 130 x 50 мм (суппорты на один, два или три поста). Этот способ имеет хорошие эстетические характеристики, но уменьшает полезную емкость КК, поскольку розетка перекрывает часть внутреннего пространства. Второй способ можно применять для КК 60 x 16 мм, 75 x 20 мм, 100 x 50 мм и 105 x 50 мм. При этом полезная емкость КК не уменьшается, но из-за того, что суппорт выступает над поверхностью крышки КК, риск механического повреждения розетки возрастает. Третий способ установки лишен недостатков первых двух. При этом используется один и тот же универсальный суппорт (он подходит только для коробов шириной менее 100 мм). Суппорт незначительно выступает над поверхностью стены, и розетки не занимают внутренний объем короба. Недостаток этого способа – большая трудоемкость монтажа, поскольку суппорт нужно дополнительно прикрепить к стене.

Кабельные каналы под брендом NTSS производятся на территории РФ на современном оборудовании из отечественного сырья. Материал, из которого изготавливаются КК, устойчив к воздействию влаги, ультрафиолета, агрессивных сред, нетоксичен. Срок эксплуатации КК и аксессуаров к ним – не менее 30 лет.

Проволочные лотки

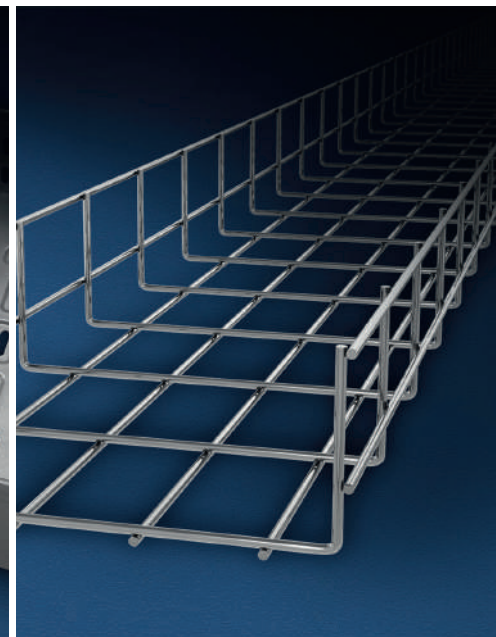
Второй вид кабеленесущих систем, производимых под брендом NTSS, – это проволочные лотки. Их преимущества перед другими типами металлических лотков известны:

- простая и быстрая сборка, требующая минимум принадлежностей и аксессуаров – поворотные элементы и разветвления можно реализовать прямо на месте монтажа, это выполняется одним человеком, имеющим кусачки для резки проволочного лотка и гаечный ключ;
- хорошая вентиляция, способствующая естественному охлаждению кабелей и предотвращающая накопление пыли и грязи;
- обзор и легкий доступ к любому участку проложенных кабелей;
- отсутствие острых углов и кромок, которые могли бы повредить кабель;
- небольшой вес лотков.

EMILINK производит лотки из стальной оцинкованной проволоки (диаметром 3,8 мм и 4,8 мм) нескольких типов исполнения для разных условий использования:

1. Гальваническое цинкование. Основой этой технологии является электрохимический процесс осаждения цинка из электролитического раствора на лоток, подключенный к отрицательному полюсу источника питания. Этот тип покрытия подходит для использования внутри помещений.

NTSS



2. Цинкование методом Сендзимира. Проволока (или листовая сталь, если речь идет о производстве листовых лотков) в горячем состоянии прокатывается через ванны с расплавленным цинком. Этот тип покрытия подходит для использования внутри помещений, а также под навесом на открытом воздухе.

3. Горячее цинкование. Полностью готовое изделие окунается в расплавленный (при температуре 460°C) цинк. Данный тип покрытия рекомендуется для использования в производственных помещениях, на химических заводах, в бассейнах и ремонтных доках.

4. Хромникелевая нержавеющая сталь AISI 304. Эта сталь обладает стойкостью к атмосферной и почвенной коррозии. Данный тип лотков рекомендуется использовать в агрессивных средах на предприятиях пищевой, металлургической, химической и фармацевтической промышленности, в медицинских учреждениях и т.п.

5. Порошковая окраска. Готовая продукция покрывается в электростатическом поле краской в виде порошка, а затем выдерживается в печи при температуре 200°C.

Специальные исполнения расширяют возможности использования проволочных лотков в агрессивных средах. Большой ассортимент типоразмеров (ширина основания от 60 мм до 600 мм, высота стенки от 30 мм до 100 мм, длина лотка 3000 мм) позволяет удовлетворять любые пожелания заказчиков. В систему производимых EMILINK проволочных лотков входит широкий ассортимент аксессуаров, повышающих надежность соединения лотков, облегчающих и ускоряющих монтаж. Это безвинтовой и перфорированный соединители, одинарный и двойной винтовые соединители, настенно-напольные кронштейны для прокладки кабелей под фальшполом, прямые подвесы для монтажа лотка на шпильках, настенные кронштейны и т.п.

Перфорированные лотки

Третий вид кабеленесущих систем NTSS – перфорированные лотки. У них есть два преимущества перед проволочными лотками:

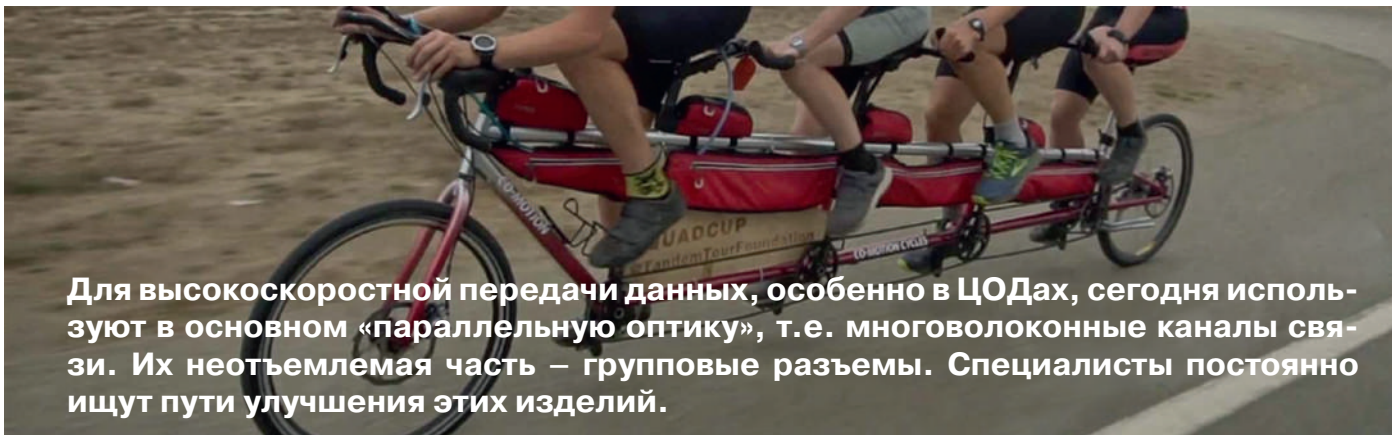
- большая нагрузочная способность;
- большая защищенность проложенных в них кабелей от внешних воздействий.

Перфорированные лотки производятся из стали толщиной 0,55–2 мм в тех же типах исполнения, что и проволочные (за исключением гальванического цинкования), а также могут быть изготовлены из нержавеющей стали марок AISI 316 и AISI 430. Лотки имеют основание шириной от 50 мм до 600 мм, стенку высотой от 30 мм до 300 мм. Прямые секции (длина одной секции – от 2000 мм до 6000 мм) соединяются между собой вводом одной секции в другую на 35 мм. Для соединения потребуются только стандартные резьбовые крепежные изделия М6. Стенка секции имеет округлый замок, который позволяет легко защелкнуть на лотке крышку и не повреждает кабель. Перфорация лотков с выдавкой создает дополнительное ребро жесткости, что увеличивает их несущую способность. Для всех размеров лотков существуют разнообразные аксессуары: горизонтальные, вертикальные (внутренние и внешние) и Т-образные углы, боковые отводы и переходники.

Для монтажа имеется большой выбор кронштейнов, потолочных подвесов, стоек, монтажных профилей и креплений, позволяющих проложить кабельную трассу в горизонтальной и вертикальной плоскостях при настенном, потолочном и напольном размещении в помещениях с конфигурацией любой сложности.

На все кабеленесущие системы NTSS (кабельные каналы, проволочные и перфорированные лотки) имеются российские сертификаты, подтверждающие высокое качество продукции группы компании EMILINK.

Направления совершенствования групповых оптических разъемов



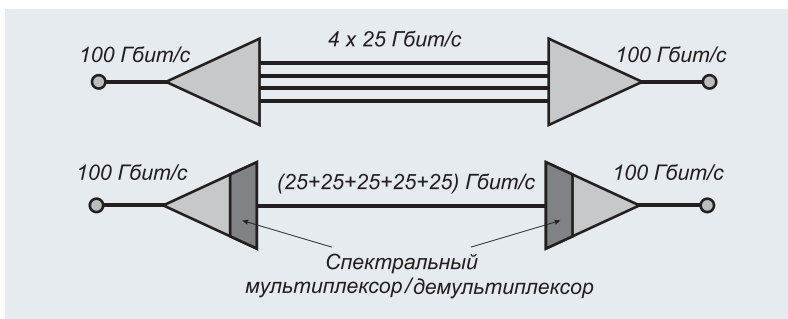
Для высокоскоростной передачи данных, особенно в ЦОДах, сегодня используют в основном «параллельную оптику», т.е. многоволоконные каналы связи. Их неотъемлемая часть – групповые разъемы. Специалисты постоянно ищут пути улучшения этих изделий.

Андрей Семенов,
профессор,
МТУСИ

Для информационного обмена со скоростью 100 Гбит/с и выше быстродействие современной электроники оказывается недостаточным, что вынуждает прибегать к параллельной передаче. В каналах связи машинных залов ЦОДов используются два функционально идентичных варианта параллельной передачи (рис. 1). Несмотря на удобство спектрального мультиплексирования с точки зрения эксплуатации, пространственное мультиплексирование из-за лучших стоимостных показателей распространено значительно шире. Соответственно в составе кабельного тракта должен присутствовать групповой (многоканальный) разъем.

В СКС функции нормативного разъема параллельных оптических трактов возложены на МРО, характеристики которого на международном уровне зафиксированы стандартом IEC-61754-7. На практике гораздо чаще применяется его усовершенствованный вариант МТР, полностью совместимый с прототипом по посадочным местам. Профильные нормативные документы не запрещают применять разъемы других типов, что оставляет простор для перспективных разработок.

Рис. 1. Схемы параллельной передачи на примере скорости 100 Гбит/с: на основе пространственного мультиплексирования (вверху) и спектрального уплотнения (внизу) ▼



Целесообразность модернизации групповых разъемов

Разъем МРО построен по трехкомпонентной схеме и разработан на базе соединителя МТ, который исходно предназначался для внутриблочного монтажа различной радиоэлектронной аппаратуры и компьютерной техники. Этим обстоятельством определяется наличие у соединителя ряда недостатков, исправление которых в существующей конструкции физически невозможно. Фактически к наконечнику МТ был лишь добавлен движковый механизм типа push-pull для фиксации вилки в проходной розетке.

Главные слабые места МРО/МТР:

- несимметричность соединителя по вилкам вследствие применения пары выравнивающих штифтов, встроенных в армирующий наконечник;
- трудность обеспечения физического контакта торцевых поверхностей сращиваемых световодов из-за применения группового армирующего наконечника;
- сложность поддержания полярности формируемого тракта;
- эксплуатационная капризность.

Последний недостаток обусловлен целым рядом факторов. Во-первых, нормы стандартов на допустимые потери в параллельных оптических кабельных трактах достаточно жесткие (см. таблицу). Это, в частности, приводит к отсутствию запасов и усложняет процесс сертификационного тестирования. Во-вторых, из-за плоской формы наконечника МТ при его плавающей установке приходится увеличивать усилие нажимной пружины с 8–12 Н, типовых, скажем, для LC и SC, до 20 Н, что сопровождается усиленным из-

носом оптически активных поверхностей волокон, ростом потерь и обратных отражений.

Сюда же добавляется сложность очистки торцевой поверхности М-варианта наконечника МТ с центрирующими штырьками, а также смены гендерности и полярности отдельных вилок при возникновении такой необходимости.

Обеспечение полярности параллельных трактов

Проблема полярности в разъемах МРО/МТР возникает из-за рядного расположения волокон в армирующем наконечнике, вследствие чего порядок нумерации передающих и приемных волокон оказывается инверсным. Основное средство решения этой проблемы – двухрядное размещение волокон в разъеме и их раскладка по прямой схеме стандартов СКС в коммутационном шнуре и стационарной линии. Такой прием применяется как в изделиях с моноблочным наконечником, так и в наборных вилках новых конструкций, что позволяет формировать простые тракты передачи по известной схеме трех скрещиваний.

Двухрядное расположение волокон по посадочным местам моноблочного наконечника и их нумерация с привязкой к отдельным приемникам Rx и передатчикам Tx сетевого 16-канального параллельного оптического интерфейса (рис. 2) в серийной продукции применяются в разъеме МХС.

Радикальное отличие изделий SN (Senko-Nano компании Senko) и MDC (Mini-Duplex компании US Conec) от МРО/МТР заключается в том, что групповая вилка может собираться прямо на объекте монтажа из двух или четырех дуплексных, которые для этого вставляются в штатную пластиковую обойму с рычажным фиксатором. Это было сделано для того, чтобы упростить построение популярных при формировании сетевых структур конфигураций port trunking (например, подключения четырех 100-гигабитных трансиверов к одному 400-гигабитному). Соблюдение требуемой полярности в этом случае не достигается автоматически и требует определенных усилий со стороны системного администратора с соответствующим уровнем знаний. При установке вилки одного конца на n-ю позицию обоймы ($n = 1 \div 4$) вилка противоположного конца должна устанавливаться на позицию 5 – n соответствующей обоймы.

Решение проблемы гендерности многоканальных разъемов

Необходимость учета гендерности классического МРО/МТР определяется его конструкцией, предусматривающей сращивание в розетке двух разнотипных вилок: одна из них имеет па-

Тип интерфейса	Год утверждения	Спецификация	Длина тракта, м	Допустимые потери, дБ
1G Ethernet-1000Base-SX	1998	IEEE 802.3z	550	3,56
10G Ethernet-10GBase-SR	2003	IEEE 802.3ae	300 (OM3) 490 (OM4)	2,6 (OM3) 2,9 (OM4)
40G Ethernet-10GBase-SR4	2010	IEEE 802.3ba	100 (OM3) 150 (OM4)	1,9 (OM3) 1,5 (OM4)
100G Ethernet-10GBase-SR10	2010	IEEE 802.3ba	100 (OM3) 150 (OM4)	1,8 (OM3) 1,5 (OM4)

ру центрирующих штифтов, которые входят в соответствующие направляющие отверстия второй вилки.

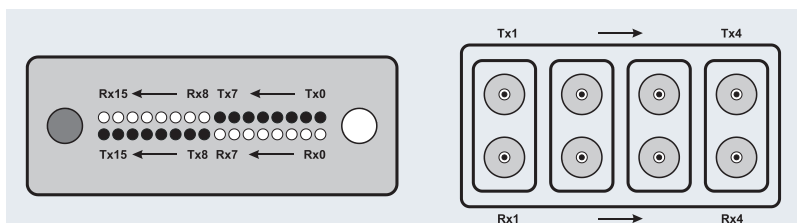
Исторически первым способом устранения этого недостатка были конструкции, которые допускали переход от F-вилки (с отверстиями) к М-вилке (со штырьками) прямо в процессе эксплуатации за счет установки пары этих штырьков на общей крепежной обойме. Обойма допускала перемещение в осевом направлении вилки и фиксировалась в одном из двух крайних положений с помощью простейших защелок. Известно несколько изделий, обеспечивающих относительно простой переход от F-вилки к М-вилке и обратно (например, PanMPO компании Panduit).

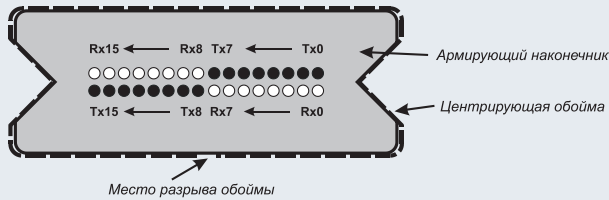
Второй способ основан на механической «симметризации» вилок панельной и кабельной частей разъема за счет того, что каждая из них содержит только один направляющий штырек, входящий в соответствующее отверстие на противоположной стороне армирующего наконечника. Для обеспечения взаимодействия элементов разъема при сборке соединителя вилки разворачиваются на 180° друг относительно друга. Ошибка при подключении невозможна из-за несимметричной формы вилки, фиксирующая защелка которой вынесена на одну из узких боковых сторон корпуса. Таким образом, способ применим только к разъемам с двухрядной раскладкой волокон в общем армирующем наконечнике. Несимметричные по штырькам вилки предлагались ранее для МРО, в серийной технике подобная структура использована в изделии МХС.

Известна также конструкция МРО-подобного разъема трехкомпонентного типа, которая отличается применением классической схемы выравнивания на основе разрезного центриатора. Сам центриатор имеет довольно сложную форму и штатно смонтирован в розетке. В собранном состоянии разъем обеспечивает взаимную юсти-

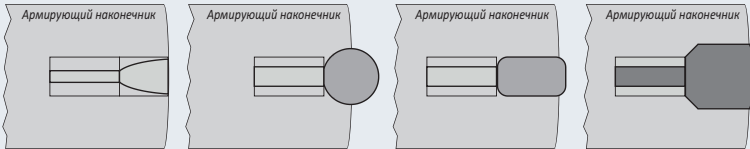
▲ Базовые параметры высокоскоростных волоконно-оптических интерфейсов Ethernet

Рис. 2. Схема раскладки волокон в центрирующем наконечнике группового оптического разъема МХС (слева) и в сборке дуплексных разъемов SN и MDC ▼

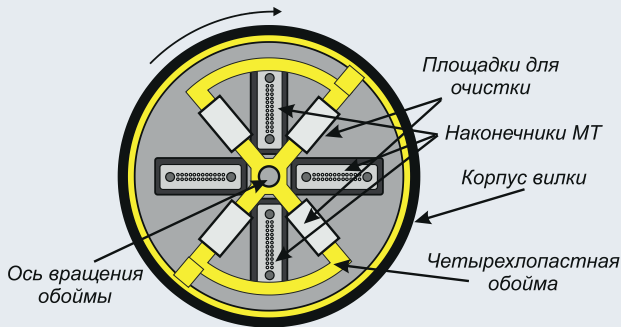




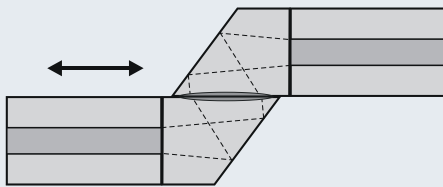
▲ Рис. 3. Схема центрирования МРО-подобного группового армирующего наконечника с помощью пружинящей обоймы



▲ Рис. 4. Варианты реализации оптических элементов разъемов с расширением луча контактного типа



▲ Рис. 5. Схема разъема SWK



▲ Рис. 6. Схема реализации оптической контактной шины

ровку вилок за счет плотного охвата и взаимодействия своими рабочими элементами с двумя треугольными вырезами на узких боковых сторонах армирующих наконечников, которые обычным образом вводятся в розетку с двух сторон (рис. 3). До серийного выпуска данное решение доведено компанией Sumitomo Electric, продвигающей его под торговой маркой AirEB.

Технология расширения луча

Расширение луча применяется в так называемых линзовых разъемах и впервые была использована в информационной системе европейских высокоскоростных железнодорожных экспрессов InterCity, где на основе этих разъе-

мов были реализованы межвагонные соединения. Технология в несколько раз увеличивает эффективную площадь оптически активных поверхностей элементов разъема, что пропорционально снижает величину потерь, вносимых частицами загрязнения.

Фокусирующий элемент разъема с расширением луча в известных конструкциях всегда встраивается в вилку, он может походить на классическую линзу или иметь иную форму (рис. 4).

Разъем может быть выполнен по традиционной (с физическим контактом оптически активных поверхностей вилок) или конструктивно несколько более сложной бесконтактной схеме. Последняя отличается нанесением на оптически активные поверхности дополнительного покрытия, подавляющего обратные отражения. Сильная сторона бесконтактной схемы – возможность уменьшения до 3 Н усилия, создаваемого нажимной пружиной. Это преимущество наиболее ярко проявляется в многоволоконных разъемах.

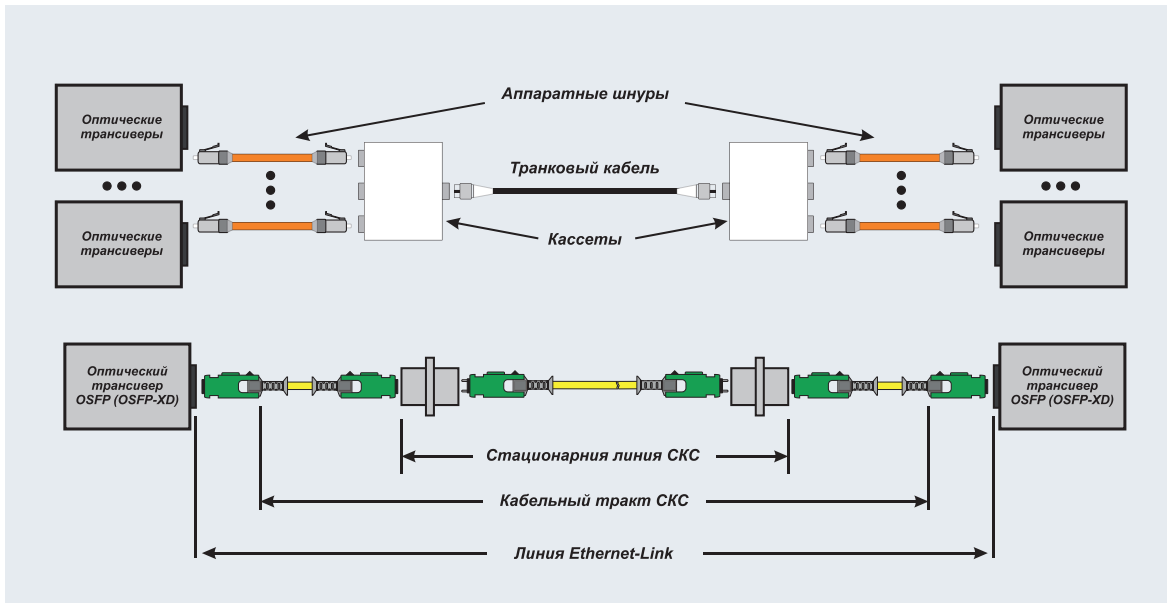
Автоматическая очистка оптически активных поверхностей

В процессе эксплуатации кабельной системы оптически активные поверхности волокон неизбежно загрязняются, в частности, из-за несоблюдения правил обращения с элементами соединителя и их подключения друг к другу. Кроме того, на них осаждаются частицы пыли, которые пусть в небольшом количестве, но обязательно присутствуют в воздухе.

Стандартные и перспективные типы оптических разъемов не содержат штатных элементов механической защиты торцевых поверхностей наконечников (крышек и заслонок). Конструкции, в которых этот недостаток устранен, не получили широкого распространения.

Другой подход – автоматическая очистка, выполняющаяся в момент подключения вилки к розетке. До уровня готового продукта доведены две разработки, различающиеся схемой рабочей процедуры.

Соединитель SWK компании Sumitomo Electric реализован на классических армирующих наконечниках МТ, расположенных крестом вокруг центральной оси (рис. 5). На этой же оси закреплена подпружиненная подвижная четырехлопастная крыльчатка с мягкими очищающими подушками на внутренних обращенных к наконечникам сторонах лопастей. При подключении вилки к розетке крыльчатка за счет взаимодействия с соответствующими неподвижными элементами корпуса вилки поворачивается примерно на 90°. В результате бокового скольжения подушки по торцевой поверхности наконечника



◀ Рис. 7. Схемы формирования стационарных линий на основе модульно-кассетного решения (сверху) и по классической схеме (снизу)

оптически активные поверхности волокон довольно эффективно очищаются от загрязнений.

Соединитель SWK интересен также тем, что в одном из его вариантов используются редко встречающиеся на практике наконечники МТ с трехрядным расположением световодов.

Еще одно решение для очистки оптически активных поверхностей предложено компанией ЗМ. В основу ее оптического разъема EVO (Expanded Beam Optical Interconnect) положен часто используемый в электрических соединителях принцип контактной шины. При подключении вилки к розетке самоочистка поверхности происходит за счет того, что контактный элемент просто сдвигает частицы загрязнения в сторону. Для реализации собственно оптического контакта в разработке применен поворот лучей на 90° (рис. 6). Правильность ориентации вилки при подключении гарантируется явно выраженной асимметрией передней поверхности корпуса, которая позволяет визуально быстро определить ее правильное положение.

Моноблочные групповые соединители с индивидуальными наконечниками

Стационарные линии кабельной системы строятся по модульно-кассетной схеме. Это, скорее, вынужденное решение для упрощения текущей эксплуатации СКС. Кроме того, появление в составе цепи передачи сигналов двух дополнительных разъемов затрудняет соблюдение норм по вносимым потерям.

Ситуацию можно исправить отказом от МРО/МТР в пользу моноблочных разъемов новых типов, реализующих схему Base8 и построенных на индивидуальных установленных по плавающей схеме наконечниках диаметром 1,25 мкм. При

этом плавающая индивидуальная установка наконечников гарантирует вносимые потери в premium-варианте на уровне 0,05 дБ. Дополнительное преимущество такого дизайна – возможность повысить скорость передачи до 1,6 Тбит/с. Линии традиционной конструкции и построенные с привлечением разъемов новых типов функционально аналогичны и за исключением внутренней интерфейсной части одинаковы (рис. 7).

На рынке представлены две разновидности изделий, реализующих эту концепцию: ассIAIM американского отделения французской компании Legrand и SN Uniboot японской компании Senko. В американском варианте, который ориентирован на транковые кабели, корпус разработан полностью с нуля. Прототипом японского соединителя стало дуплексное изделие SN, отдельные вилки которого фактически встроены в новый моноблочный корпус.

Идея этих соединителей фактически развивается на новом технологическом уровне те конструктивные решения, которые применила немецкая компания Euromicron при создании разъема URM.

■ ■ ■

Потребительские качества групповых разъемных соединителей совершенствуются достаточно быстро по различным не связанным между собой направлениям. Основные усилия разработчики прикладывают к соблюдению полярности и уменьшению вносимых потерь модульно-кассетных решений. В уже выполненных разработках наиболее серьезные конструктивные недостатки стандартного соединителя МТР/МРО устранены. Доступные на рынке образцы разъемов обеспечивают скорость до 1,6 Тбит/с, что позволит им не устареть морально по меньшей мере до 2030–2035 гг. ИКС

«Гиперлайн» выходит в премиум-сегмент

Научно-производственное предприятие «Гиперлайн», ведущий поставщик СКС, объявило о создании нового бренда для премиум-сегмента рынка. Подробности рассказывает Александр Брюзгин, директор департамента по работе с ключевыми заказчиками.



– Как «Гиперлайн» начинает 2023 г.?

– Начинаем интересно. Сейчас НПП «Гиперлайн» присутствует на рынке с двумя брендами – Hyperline и WRline, и на текущий год мы запланировали выход в премиум-сегмент рынка с новым брендом. Уточню, что речь не о расширении ассортимента, не о какой-либо дополнительной линейке решений, которые у нас уже есть. Мы выводим на рынок новый полноценный бренд для премиум-сегмента с новыми характеристиками.

– Что подтолкнуло к созданию нового бренда?

– НПП «Гиперлайн» – один из ключевых российских разработчиков и производителей систем для цифровой инфраструктуры. Мы стараемся инвестировать не только в расширение производства, но и в собственные разработки.

– Но настроения на рынке сейчас достаточно пессимистичные?

– К сожалению, да. У большинства сложилось мнение, что уход крупных западных компаний с их патентами и разработками приведет к технологическому «откату» отрасли – мол, мы сейчас все откатимся лет на пять назад. «Гиперлайн» с таким подходом не согласен. Мы всегда выступали за развитие, и наш новый бренд как раз нацелен на развитие и производства, и самого подхода к бизнесу. Он подразумевает новый уровень сервиса, взаимоотношений с заказчиками.

– А качество?

– Продукция под брендом Hyperline на рынке без малого 30 лет, мы даем 25-летнюю гарантию на СКС, и эту гарантию уже можно проверить: за весь период работы у нас не зафиксировано ни одного гарантийного обращения.

Так что для нас качество продукции – это минимальное условие вхождения в премиальный сегмент рынка. Кроме того, наша тестовая лаборатория, департамент инноваци-

онных разработок не просто тестируют продукцию. Они предлагают решения, превосходящие требования стандартов отрасли. Но в новом сегменте колоссальную роль играет особый комплекс товаров и услуг, которые нужны для выполнения специфических требований крупных заказчиков, обеспечения характеристик, индивидуально подобранных для каждого клиента.

– Кто будет управлять новым брендом?

– Для этого мы создали департамент по работе с ключевыми заказчиками. Его задача – войти в премиум-сегмент с новым брендом. Наша цель – занять лидирующее положение на рынке, обеспечить долговременное продуктивное партнерство с нашими ключевыми заказчиками – крупнейшими ИТ-потребителями и интеграторами России.

Наша миссия – предложить рынку принципиально новые решения, новые сервисы, которые будут наилучшим образом отвечать потребностям крупных заказчиков.

Наша цель – занять лидирующее положение на рынке, обеспечить долговременное продуктивное партнерство с ключевыми заказчиками – крупнейшими ИТ-потребителями и интеграторами России.

– О каких решениях идет речь?

– Прежде всего о решениях для ЦОДов. Такие решения должны отличаться максимальной производительностью, высокой и сверхвысокой плотностью в сочетании с удобством работы и надежностью.

Во-первых, производительность. Мы уже готовы продемонстрировать решения для скоростей передачи данных 100, 200 и 400GbE, а также обеспечить поддержку высокопроизводительных систем SAN вплоть до 128G Fiber



Решения для ЦОДов от НПП «Гиперлайн»



Channel. И скоро сможем предложить системы для 800GbE (как развитие 400GbE), это реальная перспектива.

Во-вторых, высокая плотность. Сейчас в отрасли принята плотность 144 волокна на 1U. Но в ближайших планах у нас 288 волокон. Удвоения плотности оптических соединений можно достичь за счет применения новых миниатюрных коннекторов. Как вы знаете, сейчас отрасль СКС разделилась на два больших лагеря – сторонников миниатюрных коннекторов Senko и сторонников US Cones. Мы уже длительное время тестируем оба типа и планируем на цодовском мероприятии «ИКС-Медиа» в сентябре продемонстрировать полное решение на одном из этих вариантов.

Но мы прекрасно понимаем, что реальный ЦОД – это не только плотность соединений. Здесь важно все: скорость, плотность, время и удобство монтажа. Поэтому, например, мы стремимся сделать так, чтобы в нашу оптическую полку на 144 волокна можно было устанавливать кассеты формата Base8, Base12 и Base24 одновременно. Другой пример нашего внимания к монтажу СКС в ЦОДах – это применение коннектора MPO с воздушным зазором, который менее чувствителен к пыли, что в условиях реального строящегося ЦОДа позволяет выиграть время без потери качества.

По данным нашей внутренней аналитики, российский рынок СКС в 2022 г. продемонстрировал падение на 16% в денежном выражении относительно 2021 г. Мы также видим структурные изменения спроса на рынке СКС: если раньше на выбор влияли такие факторы, как цена на компоненты определенных брендов и их наличие, то сейчас больше внимания уделяется способности вендора защищать своих партнеров в проектах, обосновывать не только соответствие продукции ТЗ, но и экономический эффект от приме-

продукты доводить до рынка. Сейчас мы готовы сделать следующий шаг и сфокусироваться на цифровых решениях.

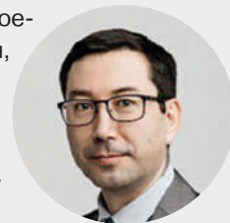
– **Речь только о новом бренде?**

– Нет, речь идет обо всех наших брендах. Наши основные задачи – наладить кроссфункциональное взаимодействие между брендами, обеспечить омниканальность.

– **Что это будет означать на практике?**

– Мы должны гарантировать нашему клиенту бесшовный опыт в потреблении решений, которые поставляем. Если речь о технологической корпорации, значит, мы обеспечим премиум-решения от нового бренда для ее частного облака и ЦОДа, потому что там обрабатывается информация, критически важная для бизнеса клиента. Затем мы можем поставить решения Hyperline для офисов, где потребителям необходимы надежность и удобство, и наконец, предложить бюджетные решения на базе продукции нашего бренда WRline для столовых, кафе, складов. Это разные бренды и разные технические решения, но для клиента мы создадим бесшовный опыт, он не будет чувствовать, где заканчивается один бренд и начинается другой. Будет у него проект на десять портов WRline или проект на сто тысяч портов на базе СКС нового премиального бренда, он получит тот же

решения того или иного решения для построения СКС. Учитывая эти и прочие факторы, в 2023 г. мы будем адаптировать свои продукты к ключевым сегментам потребления, разрабатывать решения и услуги, более точно соответствующие запросам наших партнеров и заказчиков.



Рустам Сагитдинов,
директор департамента стратегического маркетинга

Еще одно существенное отличие нового бренда от других предложений на рынке – его целостность: мы задумали премиальный продукт, канал и сервис. Мы знаем паттерны потребления наших ключевых заказчиков и знаем, что для них важна системность.

– **Кто, на ваш взгляд, будет основным потребителем?**

– В рамках нового бренда мы готовы предложить решения для потребителей, у которых ИТ-инфраструктура является основным средством производства. Сюда можно отнести крупные финансовые корпорации, технологические компании, крупных телеком-операторов и т.д. Для них ИТ-инфраструктура критически важна.

Создать качественную цифровую инфраструктуру, используя точечные поставки и имея такие проблемы с логистикой, какие сейчас существуют в рамках параллельного импорта, невозможно.

– **Насколько реально внедрение инноваций в новых условиях?**

– Суть – в смещении фокуса с продуктов на решения. Сейчас важно понимать, какое решение мы предложим ВПК, какое – сектору недвижимости, промышленному строительству, что специфического сможем предоставить РЖД. Мы научились делать качественные надежные продукты и создали эффективную партнерскую экосистему, чтобы эти

сервис, то же качество и то же внимание со стороны НПП «Гиперлайн» – мы создаем омниканальность и именно с этой точки зрения говорим об отраслевых решениях.

– **Полный охват?**

– Да, мы нацелены на разработку полного комплекса решений и полного спектра услуг технического, гарантийного и информационного сопровождения.

При всем уважении к ушедшим брендам, они не могли и не могут обеспечить кастомизированный сервис. У них у всех в России были торговые представительства с весьма ограниченными возможностями. А их центры разработки, производства и основные склады находились за 10 тыс. км от российских клиентов. Все это делало невозможным оказание требуемых услуг. А мы – российский разработчик и производитель, мы рядом. Мы можем кастомизированно выполнить оптимизацию и замещение оборудования ушедших брендов все в том же бесшовном сервисе, особенно для ЦОДов. Этот сервис включает в себя тестирование, качество и поставки вплотную к потребителю – бесшовный сервис 360 градусов. Так что ждите от нас новостей!

Hyperline

www.hyperline.ru



Домен здоровья

Николай Носов

Цифровизация поликлиник и интеграция медицинских систем позволят выработать оптимальные решения в сфере здравоохранения благодаря качественному сбору первичных данных и их анализу с помощью систем искусственного интеллекта.



Первичное звено

Цифровизация разных сегментов экономики идет неравномерно. По уровню внедрения информационных технологий лидируют банки, не сильно уступают им СМИ, а вот медицина, как заявил на городском форуме профессионалов «Моя поликлиника» председатель совета Фонда развития цифровой экономики Герман Клименко, «на последнем месте». Один из тормозящих факторов — трудности сбора первичной информации. Однако, если нет данных для обучения системы искусственного интеллекта, не будет и решений, помогающих врачу при постановке диагноза и назначении лечения. Без первичных данных нельзя оценить скорость распространения заболевания по стране, правильно спланировать закупку лекарств, подготовить места в стационарах, выявить факторы, влияющие на болезнь, и разработать профилактические мероприятия.

В регионах внедрение информационных технологий идет по-разному. Лидирует Москва, в которой на основе цифровизации полностью перестраивается система здравоохранения. С августа 2022 г. все детские медучреждения столицы работают в цифровом формате. Взрослые, по словам начальника управления мэра Москвы в Правительстве Москвы по вопросам социального развития Натальи Катаевой, перейдут на такой режим в ближайшие два года.

«Один из самых популярных у москвичей сервисов — это «Электронная медицинская карта», в котором содержится более 330 млн протоко-



лов осмотров врачей. На втором месте лабораторный сервис — там собрано около 320 млн результатов анализов», — отметил главный врач московской городской поликлиники № 220 Андрей Федорук.

В Москве реализуется масштабная, охватывающая более 200 городских поликлиник программа модернизации первичного звена здравоохранения. Стандартизирован процесс записи на прием по телефону — пациент общается с чат-ботом, который собирает первичную информацию, и врач заранее знает, с чем будет иметь дело. Электронные рецепты избавляют

Тонны бумаги уезжают в архивы. И скоро все взрослые поликлиники также будут работать в безбумажном формате.

Уже сегодня создано почти 18 млн электронных карт, доступ к которым открыт у 9 млн москвичей.

пациентов от необходимости носить с собой бланки, достаточно иметь QR-код (на смартфоне или в распечатанном виде) — и в аптеке человек получит выписанное лекарство. Телемедицинские консультации доступны горожанам с ОРВИ и подтвержденным COVID-19, они могут лечиться на дому. С февраля 2022 г. такой формат консультаций заменил 380 тыс. московских пациентов 600 тыс. визитов в медучреждения.

Конечно, не так все радужно, как рисуют на конференциях чиновники. Общение с чат-ботом не доставляет радости пациентам и нередко заканчивается ничем. Можно скачать мобильное приложение «ЕМИАС: Телемедицина», но на практике чаще всего взаимодействие ограничится телефоном. Впрочем, прогресс в цифровизации виден, запись к врачу через интернет работает, время ожидания приема в очереди сократилось. И главное — автоматизация процессов сломала предубеждения медицинских работников, показала преимущества информационных технологий и позволила наладить сбор первичных данных.

Централизация или децентрализация

Незадолго до начала пандемии в медицинских кругах шла дискуссия о принципах построения единой информационной системы здравоохранения в стране. Одна группа, которую условно можно называть «московской», выступала за централизованную унифицированную систему — использование всеми медорганизациями ограниченного набора типовых хорошо интегрированных медицинских информационных систем (МИС) — и предлагала создавать системы централизованно сверху. Но в итоге победила децентрализованная «питерская» модель — деньги на разработку МИС выделили регионам, и они, учитывая местную специфику и уровень цифровизации, осваивали инвестиции самостоятельно.

«Теперь привести региональные МИС к единому знаменателю очень сложно. Тем не менее за последние два года удалось сделать многое. Пандемия COVID-19 помогла — она продемонстрировала, для чего нужны федеральные сервисы», — пояснил заместитель министра здравоохранения РФ Павел Пугачев. Например, ког-



Наталья Катаева, начальник управления мэра Москвы в Правительстве Москвы по вопросам социального развития

да потребовалось в масштабах страны вести мониторинг заболеваемости, встал вопрос сбора информации о вакцинированных или перенесших заболевание гражданах, оказавшихся временно в других регионах и соответственно попавших в чужие базы данных. Эта информация интересовала не только региональные власти, пытавшиеся оценить уровень коллективного иммунитета, но и самих граждан, желавших получить столь нужный QR-код.



Павел Пугачев,
заместитель
министра здраво-
охранения РФ

Наша задача — создать домен здравоохранения. Уйти от отраслевых колодцев, когда есть Федеральный фонд ОМС, Росздравнадзор, Минздрав.

Объединение баз данных дает полную картину о заболеваниях в стране, освобождает человека от привязки к конкретной поликлинике. В идеале человек должен иметь возможность прийти на прием к врачу в любом регионе страны, показать свой цифровой профиль здоровья и на основании его получить курс лечения.

Создание цифрового профиля здоровья — одна из приоритетных задач, поставленных президентом перед Минздравом на декабрьском заседании Совета по стратегическому развитию и национальным проектам. Цифровой профиль включает информацию о страховке, сведения из медицинских карт, назначения врачей, список основных проблем, которые могут вызвать неприятности со здоровьем или привести к тяжелому заболеванию, госпитализации или летальному исходу. Обладателю цифрового профиля, прошедшему обследование и сдавшему анализы в одной медицинской организации, необязательно делать это еще раз при обращении в другую.

По сути, домен — единая система, объединяющая решения разных департаментов, создаваемая по единым правилам, использующая общие справочники и единый массив данных. Ядром домена должны стать электронная регистратура, федеральные реестры электронных медицинских документов, медицинских организаций, медицинских работников и единая нормативно-справочная информация.

Интеграция МИС

Работы по интеграции систем идут. В 2021 г. в законодательстве появились изменения — ГИС ОМС стала частью цифрового контура здравоохранения, ведется ее трансформация и унификация систем, находящихся в территориальных контурах. 1 декабря 2022 г. начал работать Единый регистр застрахованных лиц (ЕРЗ), и гражданам стали доступны цифровые полисы ОМС. Теперь для получения помощи в

медицинской организации достаточно предъявить паспорт или свидетельство о рождении (для детей до 14 лет).

Все новорожденные граждане с 1 декабря 2022 г. будут автоматически вноситься в ЕРЗ на основании свидетельства о рождении, выданного органами ЗАГС. Лица, получившие гражданство Российской Федерации, с того же срока будут автоматически вноситься в регистр на основании сведений, переданных органами внутренних дел.

В 2022 г. полностью в цифровом виде стали передаваться в Росгвардию медицинские справки для получения лицензии на владение оружием. Следующий шаг — выдача цифровых справок для МВД, формирующихся на основе данных обследования. За такими справками в поликлинику ходить не надо, что упрощает жизнь.

Далеко не все посещают районные поликлиники. Многие пользуются отраслевыми или коммерческими медицинскими учреждениями, ведомственными поликлиниками и больницами. В них накапливаются огромные объемы медицинских данных, которые представляют интерес как для государства, так и для граждан, желающих получить максимально полный цифровой профиль здоровья.

Работы по интеграции этих данных тоже ведутся. «Мы включили в лицензионные требования вопросы цифровизации. С 1 сентября 2021 г. независимо от того, частная медорганизация или государственная, она должна использовать медицинскую информационную систему, обеспечивающую взаимодействие с ЕМИАС. Государством за два года сформировано большое количество стандартизованных медицинских документов, которые в цифровом структурированном виде позволяют обеспечить такое взаимодействие», — пояснил П. Пугачев.

Для получения качественных структурированных данных участники системы здравоохранения должны использовать единую нормативно-справочную информацию. Разработку федеральных справочников Минздрав России ведет совместно с Департаментом здравоохранения Москвы.

Воспоминания о будущем

Население страны стареет, люди стали больше интересоваться своим здоровьем, спрос на медицинские услуги растет, врачей не хватает, а число высококвалифицированных экспертов узких специальностей можно пересчитать по пальцам. Помочь могут цифровизация, внедрение телемедицины и систем искусственного интеллекта.

Динамика цифровизации положительная. По данным П. Пугачева, количество документов,

формируемых в цифровом виде, за два года выросло в 67 раз. 95% государственных медицинских организаций внедрили МИС и начали передавать данные.

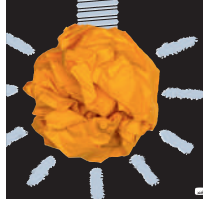
Пандемия доказала необходимость использования телемедицины, причем не только в труднодоступных уголках страны. Пока, согласно закону, первичный прием должен быть очным, но если смотреть на изменения в законодательстве опережающего нас в области телемедицины Китая, то и это требование не является бесспорным. В любом случае уже сейчас после первичного приема врач может перевести дальнейшее общение с пациентом в удаленный формат, выслушивая жалобы, корректируя лечение и выписывая лекарства. Во многих коммерческих поликлиниках это уже происходит.



И, конечно, большие надежды связаны с искусственным интеллектом. Сервисы, работающие на основе машинного обучения, уже умеют читать и понимать текст, голос и видео. За 2021 г. с помощью умного помощника «ТОП-3», разработанного компанией «СберЗдоровье» совместно с правительством Москвы, столичные врачи поставили более 3 млн предварительных диагнозов. Цифровой ассистент врача помогает анализировать жалобы пациентов во всех взрослых поликлиниках столицы. Сервис автоматически формирует направления на диагностику, благодаря чему время на оформление назначений сократилось в 10 раз.

Около 40 сервисов искусственного интеллекта в Москве помогают врачам в обработке лучевых исследований по 17 направлениям. С 2023 г. в столице вводят специальный тариф на анализ рентгеновских снимков с помощью систем искусственного интеллекта в рамках ОМС, что позволит шире внедрять технологии ИИ и не зависеть от грантовой поддержки.

По мнению Г. Клименко, в ближайшие десять лет ИИ не заменит врача, но врач, использующий ИИ, будет существенно эффективнее врача, не использующего современные цифровые технологии. Что будет через десять лет – покажет время. **ИКС**



Тренинговый центр АНО КС ЦОД

Открой новое пространство знаний о ЦОДах!

Расписание программ на 2023 год

ПОСТРОЕНИЕ ЦОД

10–12 апреля, Москва

25–26 октября, Алматы

УПРАВЛЕНИЕ ПРОЕКТИРОВАНИЕМ И СТРОИТЕЛЬСТВОМ ЦОД

17–19 мая, Москва

15–17 ноября, Москва

ЭКСПЛУАТАЦИЯ ЦОД

26–28 июня, Москва

11–13 декабря, Москва

ЭЛЕКТРИЧЕСКИЕ И МЕХАНИЧЕСКИЕ СИСТЕМЫ ЦОД

11–13 октября, Москва



Специусловия при прохождении онлайн-курсов
Подробнее уточняйте по email: info@ano-dcc.ru

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/





Российские почтовые и коммуникационные платформы: какую выбрать

При выборе коммуникационной платформы в первую очередь нужно обратить внимание на ее функциональные возможности, требуемые ресурсы, протоколы подключения, сложность администрирования и пользовательский интерфейс.

Андрей Головкин, руководитель направления по развитию отечественных решений; **Александра Залманова**, руководитель команды «Регионы РФ» департамента развития отечественных ИТ-продуктов; **Константин Остахов**, технический эксперт по российскому ПО, ГК Softline

Практически каждая организация применяет в работе программные продукты, объединяющие в себе необходимые инструменты для передачи и получения информации. Для этих целей существуют зарубежные и российские решения, а также open source-продукты. Однако приобрести зарубежное ПО сегодня стало практически невозможно, а использование свободно распространяемых продуктов связано с серьезными рисками: наличием недекларируемых возможностей; отсутствием технической поддержки и репозитория на территории России; непредсказуемостью развития функциональности; непрогнозируемыми сроками внесения изменений в продукт при выявлении уязвимостей; изменением лицензионного соглашения без ведома пользователей; отсутствием обучающих курсов.

Поэтому при выборе коммуникационной платформы мы рекомендуем компаниям обратить внимание на российские решения, входящие в реестр ПО Минцифры и нивелирующие перечисленные выше риски. В числе этих продуктов можно назвать CommuniGate Pro, Mailion, VK WorkSpace, «МойОфис Почта 2», а также RuPost от ГК «Астра», который будет интересен пользователям, желающим сохранить целостность инфраструктуры Astra Linux.

Все эти решения предполагают различные варианты размещения – на серверах заказчика или в облаке. Пользователи все чаще хотят получать такие сервисы, подобно зарубежным аналогам, по подписке, без необходимости создания собственной инфраструктуры. Поэтому коммуникационные и почтовые платформы предлагаются в том числе как SaaS-решения.

Коммуникационные платформы и их особенности

Основная проблема, с которой сталкиваются заказчики при переходе с зарубежных решений на российские, – сохранение всех сервисов, ор-

ганизация совместной работы с календарями, видеоконференциями и обеспечение надежного мобильного доступа. Зачастую также требуется наличие десктопного клиента.

«МойОфис Почта 2» – российское решение для организации электронной переписки, календарного планирования и работы с задачами, ориентированное в первую очередь на предприятия, которым нужно качественное и безопасное почтовое решение с развертыванием на собственной инфраструктуре. Для компаний с повышенными требованиями к защите информации имеется версия продукта с поддержкой российских криптоалгоритмов. Поскольку продукт строится на базе контейнеров, он может быстро масштабироваться и позволяет подключать до нескольких десятков тысяч пользователей, благодаря чему можно создавать большие отказоустойчивые системы. Продукт подойдет компаниям, которые имеют большой штат сотрудников или быстро растут. Пользователям доступны веб-, настольный и мобильный почтовые клиенты. Для государственных и академических организаций действуют специальные ценовые предложения.

Продукт «МойОфис Почта 2» можно дополнить облачным решением «МойОфис Частное Облако 2», которое предоставляет возможность совместной работы и редактирования документов в частном облаке организации. Помимо этого, в серверное решение включены встроенные средства защиты информации.

Mailion – тиражируемая корпоративная почта нового поколения, построенная на облачно-ориентированной (cloud native) микросервисной архитектуре и обеспечивающая одновременную работу до 1 млн пользователей. Благодаря микросервисной архитектуре Mailion обладает высокой отказоустойчивостью. Хранилище почтовой системы поддерживает дедубликацию данных для надежного и экономичного хранения

информации. Такое решение будет востребовано у госкомпаний и крупных организаций со штатом сотрудников более 30 тыс. человек. Отличается требовательностью к ресурсам и сложностью администрирования.

Продукт ориентирован на замену Exchange. В комплект входят серверные приложения, веб-клиент и версия для мобильных устройств. Для обеспечения бесшовной миграции с постепенной заменой зарубежного ПО на компьютерах заказчиков производитель предлагает интеграционное решение в виде надстройки для Microsoft Outlook, которое позволит пользователям продолжать работать с привычными инструментами в процессе замены ПО. Также доступна современная корпоративная система календарного планирования, которая предоставляет широкие возможности для взаимодействия пользователей, в том числе позволяет делиться событиями с другими участниками встречи.

VK WorkSpace – это коммуникационная платформа для бизнеса, разработанная VK. В настоящее время в линейку входят три продукта – почтовый сервер VK WorkMail, корпоративный мессенджер VK Teams и хранилище VK WorkDisk. Почтовый сервер ориентирован на организации от 3 тыс. пользователей и обладает широким функционалом почты и календарей. Для расширения его возможностей можно развернуть VK Teams, который позволяет проводить аудио- и видеоконференции с подключением большого числа пользователей, что важно для заказчиков, ищущих альтернативу таким продуктам, как Zoom, Microsoft Teams и Skype for business.

Платформа VK WorkSpace требует столько же серверных ресурсов и квалифицированного персонала, как и Mailion. Система может быть запущена только на больших мощностях. Для старта в отказоустойчивом режиме для 3 тыс. пользователей требуется 32 Гбайт оперативной памяти, 24 ядра виртуальных процессоров и исключительно SSD-диски. Систему достаточно сложно администрировать тем, кто ранее не работал с технологиями контейнеризации. Однако пользователей привлечет удобный интерфейс, знакомый со времен почты Mail.ru.

К преимуществам платформы можно отнести наличие удобного мобильного и десктопного приложения VK SuperApp, которое включает в себя все необходимые коммуникации: передачу почтовых сообщений, звонки, чаты, календари.

CommuniGate Pro – это коммуникационная платформа, разработанная компанией CommuniGate Systems. Она отличается малой требовательностью к физическим ресурсам. Например, для обслуживания 2500–10 000 пользователей будет достаточно двухъядерного процессора с 4 Гбайт оперативной памяти. CommuniGate Pro –

лидер российского рынка в данном сегменте по количеству инсталляций. Это решение может быть рекомендовано любой компании со штатом 25–250 000 человек. Особенность платформы – возможность интеграции со сторонними решениями. Этот продукт можно использовать с клиентами по стандартным протоколам IMAP и POP3, а также Outlook с помощью API-коннектора. Помимо этого, пользователям доступны интеграции с телефонией, с зарубежными системами и сервисами, развернутыми у заказчика.

У платформы есть собственная экосистема клиентских приложений. В лицензионный пакет входит веб-клиент, а за дополнительную плату можно приобрести мобильный и десктопный клиенты. Преимущество решения – в едином ядре, благодаря которому заказчик получает все корпоративные коммуникации, что важно для организаций, планирующих в дальнейшем наращивать функционал платформы.

Решение от CommuniGate Systems подойдет компаниям, привыкшим работать с протоколами Exchange и ActiveSync. Пользователям доступны унифицированные коммуникации, включающие возможность использования мобильных приложений, а также синхронизацию почты и календарей.

Платформа может быть интегрирована с внешними редакторами, позволяя редактировать и открывать документы в веб-интерфейсе. Система CommuniGate Pro удобна и проста для понимания с точки зрения администрирования.

Как перейти с иностранных почтовых решений на отечественные

К нам часто обращаются организации, которым требуется перейти с иностранных коммуникационных платформ на российские. Мы собрали самые частые вопросы наших заказчиков на эту тему и постараемся рассказать, что же делать в той или иной ситуации.

Перенос почты из старой почтовой системы в новую

Здесь в первую очередь нужно понимать, какая старая почтовая система использовалась в организации и по каким протоколам она может экспортировать почту. Чаще всего речь идет либо о Microsoft Exchange, либо о другой почтовой системе, способной отдавать почту по протоколу IMAP. В этом случае можно перенести почту в любую почтовую систему, будь то CommuniGate Pro, «МойОфис Почта 2», VK Workspace или Mailion. Если заказчик использовал Exchange, на котором был настроен только протокол ActiveSync, то перенести почту с почтового сервера смогут только решения от CommuniGate, у которых есть специальная утилита, позволяющая провести за-

Характеристика	Продукт			
	CommuniGate Pro	«МойОфис Почта 2»	VK WorkSpace	Mailion
Основа	C++/Perl	Postfix, Docker, MariaDB...	NGINX, S3, Docker, Tarantool...	RethinkDB, Go, Docker...
Количество почтовых ящиков	1–15 млн	1 тыс. – 30 тыс.	5 тыс. – 50 тыс.	30 тыс. – 1 млн
Кластер	+	+	+	+
Протоколы	POP3/IMAP/SMTP/ActiveSync	POP3/IMAP/SMTP	POP3/IMAP/SMTP	IMAP/SMTP
Редакторы	API	+	API	–
Сложность администрирования	Низкая	Средняя	Высокая	Высокая
Обучающие курсы	+	+	–	+
Сертификат ФСТЭК	+	–	–	–

▲ Сравнение серверных компонентов коммуникационных платформ

бор почты. Мы рекомендуем заказчикам обращаться к интеграторам, которые уже проводили такие работы и знают все подводные камни при настройке процесса миграции.

Организация работы с почтой на мобильных устройствах

Если заказчик привык работать с протоколом Exchange ActiveSync, который обеспечивает доставку почты через зашифрованный туннель, обмен календарями, контактами и задачами, то ему больше всего подойдет платформа CommuniGate Pro. С помощью протокола ActiveSync можно работать с привычными мобильными приложениями, которые уже есть на устройствах под управлением iOS и Android. Однако при желании заказчик может перейти на мобильное приложение от CommuniGate – Samoware. «МойОфис Почта 2» предлагает свои мобильные приложения для iOS и Android, чтобы работать с почтой по протоколу IMAP/SMTP и с календарными событиями и задачами по протоколу CalDav.

Если компании не требуется синхронизация контактов, календарей и задач, а нужно просто забирать почту на мобильный телефон с помощью открытого или зашифрованного протокола IMAP, то ему подойдет любая из описанных почтовых систем.

Совместная работа с календарями и задачами посредством мобильных устройств

При работе через веб-интерфейс сервера каждое из описанных выше решений позволяет отслеживать занятость, вести совместную работу с календарями, назначать мероприятия. Однако подключить к системе мобильные клиенты с

такими же возможностями смогут только CommuniGate Pro и VK WorkSpace.

При работе с корпоративной почтой на мобильных устройствах очень важна защита информации. В этом плане мы рекомендуем обратить внимание на продукт Workspad от ГК «Астра», который позволяет работать с корпоративными ресурсами (порталом, почтой или файлами) через мобильные устройства, используя защищенные каналы связи. Workspad обеспечит доступ к этим ресурсам на мобильном устройстве без риска утечки персональных данных. Например, при попытке сфотографировать документ для пересылки будет высвечиваться черный экран.

Не забудьте обучить персонал работе с новыми платформами

Еще одна сложность при переходе на российские коммуникационные платформы – отсутствие квалифицированных кадров. Поэтому важно своевременно провести обучение персонала. Раньше обучение сотрудников не стояло на первом месте, поскольку переход на российское ПО мог осуществляться плавно, сейчас же он стал насущной необходимостью. Конечно, подводные камни существуют – перенос данных, внедрение почты в действующую инфраструктуру и др. К сожалению, не для всех продуктов есть обучающие курсы. Надеемся, что в ближайшее время они появятся.



У каждого из описанных продуктов есть свои преимущества и недостатки. При выборе решения мы рекомендуем компаниям обратить внимание на масштаб собственной инфраструктуры, протоколы подключения, отказоустойчивость используемых систем, а также на сложность администрирования и наличие унифицированных коммуникаций в виде чатов и звонков.

Несмотря на различия в пользовательском интерфейсе, все описанные коммуникационные платформы сохраняют общую логику работы с почтой. Например, интерфейсы продуктов «МойОфис Почта 2» и Mailion просты и интуитивно понятны. Интерфейс CommuniGate Pro не похож на другие и требует дополнительного изучения, однако удобен в использовании. VK WorkSpace подкупает уже знакомым всем интерфейсом, некогда популярным у b2c-пользователей почты Mail.ru.

На каком бы продукте вы ни остановили свой выбор, важно грамотно провести все этапы миграции: рассчитать необходимые мощности, этапы внедрения, а также учесть архитектуру решения, переключение сервисов, обучение персонала, необходимые лицензии, дальнейшее сопровождение и поддержку. **ИКС**

Жизнь после VMware

За последние месяцы даже самые стойкие пользователи зарубежного ПО смирились с мыслью, что западные вендоры не вернуться на российский рынок и нужно искать альтернативные решения, погружаться в импортозамещение и перестраивать ИТ-инфраструктуру компаний.

*Это просто вопрос выбора и привыкания.
Дж. Джером. Раб привычки**

С одной стороны, все просто: нужно заменить то, что уже нельзя спасти, с другой – необходимо среди множества продуктов новых вендоров выбрать тот, который гарантирует стабильность работы всех сервисов. Интуитивный метод не подойдет, бизнес в трудные времена просчитывает каждый шаг и вкладывает средства только в работающие решения. Поэтому перед тем, как приступить к выбору продукта, нужно понять, какие характеристики и опции он должен иметь для бесшовной интеграции в инфраструктуру компании.

Большой резонанс вызвало прекращение работы в России разработчика программного обеспечения VMware. Более 15 лет продукты этой компании занимали 90–95% российского рынка систем виртуализации. Технологии виртуализации позволяют запускать на одном сервере несколько логических единиц – виртуальных машин, что дает возможность компаниям не покупать отдельный сервер для каждого приложения, а размещать на одной единице оборудования до нескольких десятков независимых операционных систем и корпоративных приложений, тем самым более эффективно используя ИТ-инфраструктуру. Но теперь российские компании вынуждены решать жизненно важный вопрос: как продолжать работу в условиях отсутствия продукции одного из ключевых игроков, т.е. как жить без VMware.

При выборе подходящей альтернативы в первую очередь нужно смириться с тем, что системы, идентичной решению VMware, нет. Затем следует оценить уровень техподдержки на переходный период. Ведь действующую версию продукта нужно поддерживать в рабочем состоянии до интеграции нового и переноса в него всех данных. Только после этого компания будет готова к

главному шагу – выбрать продукт, который по своим возможностям максимально приближается к решению VMware и входит в реестр российского ПО, если есть такое требование.

На какие характеристики альтернативного решения обратить внимание

Гиперконвергенция

Удобно, если платформа позволяет выбрать классическую или гиперконвергентную структуру. Плюс классической версии в том, что ее поддерживают все вендоры российского рынка. Но гиперконвергентная структура финансово более выгодна: ее легко масштабировать и она не требует дополнительных вложений в покупку специализированного оборудования для системы хранения данных. В частности, в такой структуре система хранения данных не является отдельным узлом, а каждый сервер выделяет под хранение свои жесткие диски. Также в гиперконвергентной структуре программно определяемые сети не требуют дополнительного оборудования.

Централизованное управление

Централизованное управление особенно важно для крупных дата-центров или инфраструктуры среднего масштаба, состоящей из десятков или сотен серверов. Для работы с подобными инфраструктурами предпочтительнее иметь централизованное управление. Ведь если у системы виртуализации такого функционала нет, то, скажем, при тестировании на каждом узле виртуализации нужно будет повторять действие, уже выполненное на соседнем узле. Соответственно объем работы значительно возрастет.

Живая миграция

Перед построением больших отказоустойчивых кластеров нужно не только обеспечить миграцию между хостами виртуализации, но и понять, какое количество информации теряется в этих миграциях между хостами. Принципы, по которым осуществляется миграция, в разных решениях различаются. Из-за этого заказчик может потерять нужную информацию, например, при сбое сервера в момент пиковой нагрузки.

Виталий Попов,
директор
департамента
реализации
инфраструктурных
проектов, Softline

* Самые смешные рассказы/The Best Funny Stories. «Издательство АСТ», 2019.

Средства резервирования

Следует выбирать решение, совместимое со средством резервного копирования, чтобы система виртуализации могла с ним взаимодействовать, а заказчик при внедрении новой системы понимал, как ему в дальнейшем делать бэкапы своих виртуальных машин. Идеальным будет вариант, когда средство резервного копирования поддерживает и исходную, и целевую платформы виртуализации. Не все существующие системы виртуализации интегрируются со всеми доступными средствами резервного копирования и ими поддерживаются. Но списки совместимости, скажем, систем RuBackup и «Кибер Бэкап», постоянно расширяются.

Важный момент, который стоит учесть при выборе решения: встроенное средство резервирования, если такое предоставляет платформа, финансово выгодно, поскольку не требует дополнительных затрат. Но оно может оказаться несовместимым с другими частями инфраструктуры, что приведет к децентрализации резервного копирования, т.е. нужно будет иметь два инструмента.

Документация

Большинство вендоров заботятся о качестве предоставляемой документации, но есть и такие, кто детальное описание откладывает на потом. С точки зрения пользователя важно, чтобы все функциональные возможности и особенности решения были тщательно описаны, только в этом случае он сможет их задействовать в дальнейшем.

Актуальная ситуация на рынке диктует отказ от лишних опций и дорогостоящих функций в пользу экономически выгодных решений. Зачастую продукт на 30% состоит из базовых опций и на 70% – из дополнительных, которые используются редко. Поэтому перед покупкой и интеграцией продукт следует внимательно изучить. И здесь большую роль играет наличие подробной документации.

Алгоритм бесшовного переноса системы виртуализации

После того, как заказчик решил на внедрение новой платформы виртуализации, нужно

убедиться, что инфраструктура предприятия перейдет из состояния А в состояние Б без потерь.

Опишем методику, следование которой позволяет в 99% случаев провести переход успешно. Процесс занимает один год и включает два этапа – подготовку и собственно переход (рис. 1).

Для того чтобы бизнес не парализовало в процессе перехода, за это время компании необходимо сделать пять простых шагов.

Шаг 1

ИТ-подразделению нужно ответить на три ключевых вопроса для понимания того, насколько компания готова к переходу:

- ▶ Готовы ли ИТ-специалисты отложить текущие задачи и целиком переключиться на процесс перехода?
- ▶ Способны ли сотрудники понять, развернуть и настроить новое решение?
- ▶ Понимают ли специалисты, как провести интеграцию исходной и целевой системы, и готовы ли ее осуществить?

Если ответ хотя бы на один из этих вопросов будет отрицательным, то при самостоятельном переходе есть риск потерять данные или допустить остановку бизнес-процессов. В таком случае оптимальным вариантом станет обращение к доверенному партнеру, ИТ-интегратору, который обладает достаточной экспертизой и опытом в решении подобных задач. Далее рассмотрим переход на альтернативную систему виртуализации именно с привлечением ИТ-интегратора.

Шаг 2

Команда ИТ-интегратора готовит дорожную карту (рис. 2) рекомендуемых технических мероприятий на год и план консультационного сопровождения специалистов заказчика на всех этапах перехода, включая обучение на сертифицированных курсах.

Шаг 3

Подготовительная стадия – технически сложный период, в зависимости от размера компании он потребует от ИТ-специалистов от шести до девяти месяцев работы. За это время нужно подготовить компанию к прекращению эксплуатации функционирующей системы и одновременно протестировать новую систему российского вен-



Рис. 1. ► Процесс перехода на новую систему виртуализации

Сценарий перехода инфраструктурных сервисов на российское решение 2022–2023

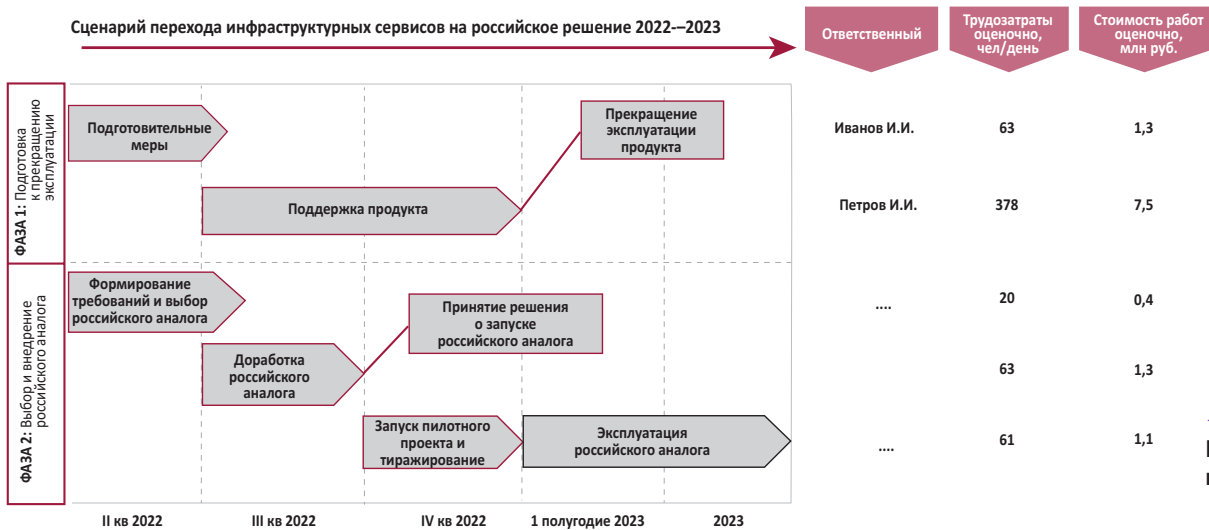


Рис. 2. Пример дорожной карты

дора. Таким образом, одновременно будут работать две платформы, старая и новая. Неактуальное решение западного вендора нужно будет поддерживать технически, а новое – интегрировать в инфраструктуру. Это поможет перейти к новому программному обеспечению без потерь.

Техподдержка решений вендоров, покинувших российский рынок, – самый частый запрос заказчиков. При выборе ИТ-интегратора для внедрения нового продукта важно заранее убедиться в его способности качественно поддерживать все решения.

Подготовительная стадия состоит из пяти этапов:

- ▶ анализ программного обеспечения;
- ▶ пилотное развертывание;
- ▶ тестирование;
- ▶ оценка совместимости с информационными системами;
- ▶ анализ результатов и планирование перехода.

Шаг 4

Переход включает в себя подготовку технического задания, выбор и внедрение российского аналога, а также его доработку в соответствии с конкретными запросами заказчика. Эти действия интегратор выполняет одновременно с подготовительной стадией, они занимают полгода. Далее следуют запуск и тиражирование российского проекта.

Переход также проходит в пять этапов:

- ▶ согласование этапов перехода;
- ▶ поэтапная реализация перехода;
- ▶ поэтапная приемка результатов;
- ▶ обучение;
- ▶ техподдержка.

Передача в промышленную эксплуатацию российского продукта и прекращение использования западного наступают примерно через десять месяцев после того, как ИТ-специалисты приступили к выполнению задачи.

Шаг 5

После завершения процесса перехода ИТ-подразделение заказчика получает новое ПО. Специалистам нужно привыкнуть к интерфейсу, а также четко понимать, как эксплуатировать решение. Для этого необходимы обучающие курсы. VMware подробные программы обучения предоставляла, но новые вендоры не все успели разработать свои курсы, причем 90% материалов посвящены базовым характеристикам продукта и не дают углубленных знаний.

Этот момент важно предусмотреть на этапе выбора доверенного партнера. Если ИТ-интегратор предоставляет ресурсы собственного учебного центра, курсы, тренеров по конкретным решениям вендоров, заказчик может быть спокоен за дальнейшую эксплуатацию продукта.

За прошедшие месяцы нишу VMware на российском ИТ-рынке заполнили достаточно зрелые отечественные системы аппаратной виртуализации. Вендоры предоставляют заказчикам широкий спектр решений для виртуализации серверов, десктопов, приложений, систем управления и обеспечения безопасности виртуальной среды, поставляют ПО и оборудование для виртуальной среды. А ИТ-интеграторы оперативно взяли под контроль техподдержку инфраструктуры российских предприятий и их полное сопровождение в переходе на импортозамещающие решения.

Кроме того, в России остались уникальные ИТ-специалисты, экспертиза которых охватывает виртуализацию серверов, систем хранения, сетей и рабочих мест. Они разрабатывают для заказчиков сценарии, которые ведут к понятным и ощутимым результатам – гибкой и динамичной инфраструктуре, минимизации расходов, реализации планов роста. Таким образом, 2022 г. очередной раз дал возможность убедиться, что кризис – это время новых возможностей. ИКС

Время постправды



Николай Носов

В распространении сфальсифицированной, недостоверной и заведомо ложной информации, или, на современном языке, фейков, нет ничего нового. Но теперь фейки все чаще становятся оружием в информационной войне. Бороться с ними можно только открытостью и правдой.

Сначала слухи передавали из уст в уста, потом добавилась печатная продукция, затем радио. Менялись и масштабы воздействия – если в Средневековье на основании слухов об использовании колдовства на костер отправляли одного человека, то работа «Радио тысячи холмов» в Руанде привела к самому эффективному геноциду в новейшей истории и за 100 дней лишила жизни около миллиона человек.

На протяжении веков развития цивилизации менялись лишь технологии и каналы доставки контента. Качественный скачок произошел в 21-м веке благодаря достижениям информационных технологий, всеобщей цифровизации и массовому распространению интернета. Теперь каждый человек имеет легкодоступный канал связи с каждым, может стать СМИ, вещать на широкую аудиторию, распространять любую, в том числе фейковую информацию.

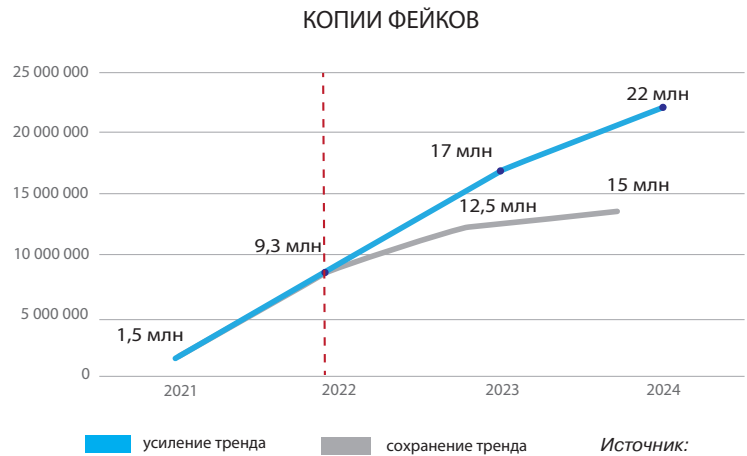
Общедоступные цифровые технологии позволяют, редактируя фотографии, видео и сканы документов, создавать правдоподобные изображения и даже дипфейки – фальшивые видео с заменой одного лица на другое. А распространители фейков могут использовать таргетированную рекламу и подгонять содержимое фейка под профиль человека, используя информацию из публикаций в интернете, чатов, мессенджеров и социальных сетей.

Начало массовому распространению фейков, как заявил генеральный директор АНО «Диалог» и АНО «Диалог Регионы» Владимир Табак при подведении итогов работы по противодействию фейковой информации, положила эпидемия коронавируса. В Сети стали появляться самые нелепые слухи – о чипировании людей Биллом Гейтсом, о том, что вакцинированные общаются с вышками сотовой связи 5G и даже притягивают металлические предметы.

Обострившаяся в феврале геополитическая ситуация и начало СВО вызвали новую волну фейков. По данным АНО «Диалог Регионы», в 2022 г. количество фейковой информации – массива ссылок, идущих за уникальным фейком, – выросло в шесть раз по сравнению с 2021 г.: с 1,5 млн до 9,3 млн (рис. 1). Причем прогнозируется дальнейшее увеличение числа фейков – до 22 млн в 2024 г.

Количество уникальных фейков прямо коррелирует с политической обстановкой в стране: наибольшее число пришлось на март – начало СВО и сентябрь – начало частичной мобилизации (рис. 2).

Массовые вбросы в интернет ложных сведений привели к тому, что люди стали скептически относиться к любой информации. Это отразилось на поисковых запросах – интерес к тематике фейков за последний год вырос на 68%.



Источник: «Диалог Регионы»

«Пользователи понимают, что наступило время постправды», – пояснил В. Табак.

Совсем не безобидное вранье

Фейки могут создаваться по экономическим мотивам, с целью обмануть аудиторию и выманить деньги, например на лечение несуществующего ребенка, или монетизировать трафик, возросший из-за уникальной фальшивой новости или подделанного медиа. Мотивы могут быть психологическими – желание повысить самооценку и авторитет автора в глазах окружающих или выставить в неприглядном виде других людей. Целью может быть и нанесение урона престижу и авторитету конкурирующей фирме на рынке или отдельному государству в глазах общества или на международной арене.

Чаще всего (61%) встречаются ложные заявления/намеренная дезинформация (рис. 3), затем идет использование архивных или постановочных видео или даже кадров из художественных фильмов, как, например, для «доказательства» геноцида мусульман в Мьянме. Больше всего недостоверной информации можно встретить в отечественных соцсетях. Практически половина всех фейковых сообщений приходится на площадки «ВКонтакте» (24%) и «Одноклассники» (21%). За ними сразу идет Telegram (20%) и лишь потом соцсети запрещенных и

Рис. 1. ▲ Прогноз роста числа фейков в 2023–2024 гг. с учетом усиления и сохранения тренда их роста

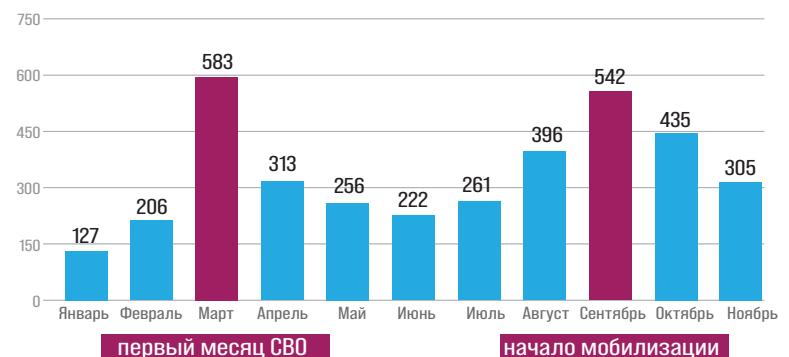
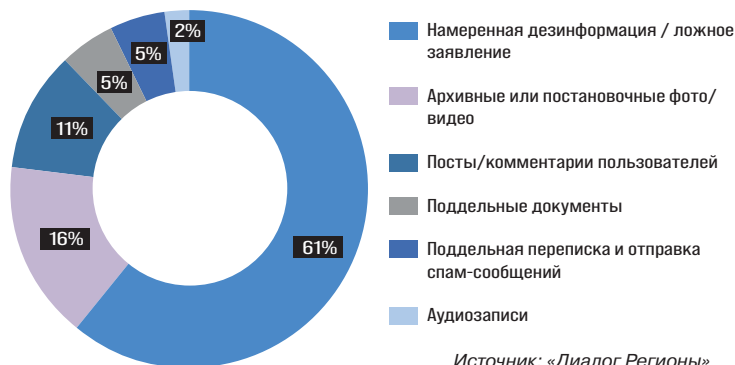


Рис. 2. Число уникальных фейков в 2022 г. ▼

Источник: «Диалог Регионы»



Источник: «Диалог Регионы»

Рис. 3. ▲
Наиболее популярные фейки

признанных экстремистскими международными компаниями, аудитория которых сильно уменьшилась из-за блокировок Роскомнадзора.

Распространение фейков, как считают 79% граждан, представляет реальную опасность для общества (рис. 4). Такие данные привела начальник управления Президента Российской Федерации по развитию информационно-коммуникационных технологий и инфраструктуры связи Татьяна Матвеева.

За слова надо отвечать

Фейки не только вводят граждан в заблуждение, но сеют панику и используются для пропаганды, становясь оружием в информационной войне. Это вызывает озабоченность государства. В цифровом обществе блогеры имеют аудиторию, зачастую превышающую аудиторию традиционных СМИ, но при этом не несут ответственности за истинность размещаемой информации. Серьезные СМИ проверяют информацию по нескольким источникам и за счет этого проигрывают в скорости блогерам в конкурентной борьбе за читателей.

Контроль над блогерами с аудиторией свыше 3 тыс. пользователей пытались ввести еще в 2014 г., внося поправки в закон «Об информации, информационных технологиях и о защите информации». К владельцам сайтов и учетных записей стали применять все ограничения,

установленные в России для СМИ. Но из-за несогласованности позиций ведомств закон так и не заработал – несмотря на выявляемые нарушения, ни одному из блогеров штраф не выпишали. В июле 2017 г. с внесением новых поправок норму отменили, но проблема осталась.

Следующая попытка контроля интернета была предпринята в 2020 г. С 01.02.2021 вступил в силу закон о самоконтроле социальных сетей (№ 530-ФЗ), в соответствии с которым интернет-площадки обязаны сами выявлять и блокировать социально опасную информацию. Новый закон тоже вызвал критику. Пользователи площадок пишут когда и что угодно, а владельцам трудно оперативно выявлять ложный или противоправный контент. Кроме того, они не всегда обладают необходимой для этого экспертизой.

Екатерина Ларина, директор департамента развития массовых коммуникаций и международного сотрудничества Минцифры России, сообщила, что рассматривается возможность введения мягкого контроля фейков. Предполагается штрафовать площадку не сразу после выявления фейка регулятором, а лишь в случае умышленного нарушения, о котором владелец знал, но мер не принял. Или же, если заявление о выявленном фейке поступило от авторизованного субъекта, например фактчекинговой платформы или СМИ, то в случае отсутствия возражений автора фейк удаляется. Если возражения есть, в спор вмешивается модератор, принимающий окончательное решение. И только при отсутствии реакции на заявление владелец площадки понесет наказание.

Чему верить, что проверить

Для выявления фейков АНО «Диалог Регионы» развернула фактчекинговый сервис «Лапша Медиа», включающий сайт (<https://lapsha.media>) с функцией проверки информации, чат-бот в «ВКонтакте», медиамониторинг и базу фейков. С момента запуска платформы поступило более 85 тыс. запросов на проверку публикаций и сообщений.

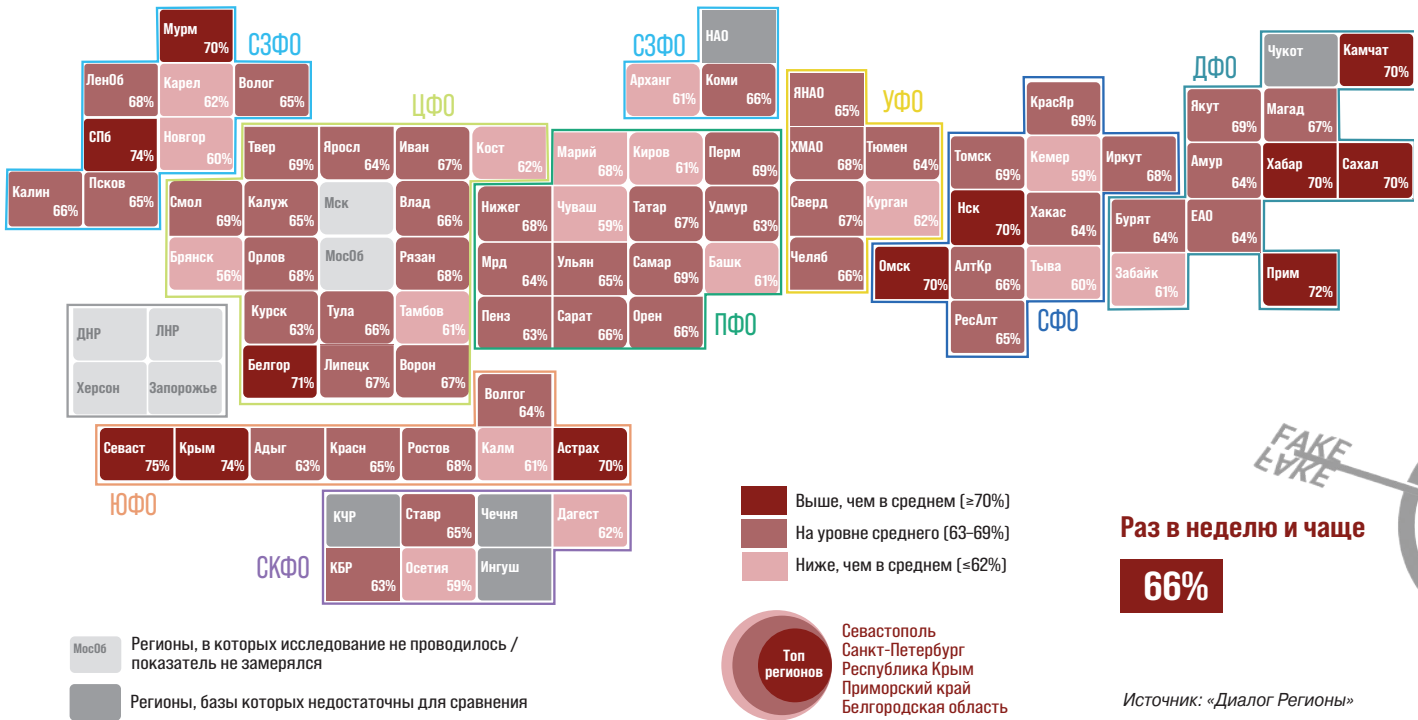
Среди партнеров сервиса «Лапша Медиа» – площадки Lenta.ru, ТАСС, 360tv и Высшая школа экономики. Мониторинг открытых источников проводится в автоматическом режиме с использованием технологий машинного обучения. Отобранные потенциальные фейки ежедневно проверяются экспертами на достоверность, и по самым значимым из них публикуются материалы.

В целом проект выглядит интересным. Правда, практическая его полезность пока не до конца понятна. Недавно увидел на сайте Lenta.ru новость: «Бегемот проглотил ребенка и выплюнул его живым». Несмотря на широко распространенное заблуждение, бегемоты не питают-

Рис. 4. ▼
Воздействие фейков на общество



Источник: управление Президента РФ по развитию информационно-коммуникационных технологий и инфраструктуры связи



ся детьми – у травоядных по-другому устроен желудок. Бегемот – опасное животное и может напасть на человека. Но не для того, чтобы проглотить, а для того, чтобы растоптать или перекусить, что иногда и происходит. Так что публикация смотрится как фейк. Послал с редакционного адреса на сайт «Лапша Медиа» запрос на проверку публикации, указал ссылку, но не получил ответного сообщения, что заявка принята и находится в обработке. Впрочем, через пять часов получил ответ, что это не фейк, и ссылку на первоисточник – The Daily Telegraph. В английском издании, правда, говорится не «проглотил» (оказался в желудке), а «оказался в больших челюстях животного». А это большая разница. Но, видимо, умышленное искажение истины в заголовке для привлечения трафика фейком не считается. На запрос с личного адреса о проверке публикации на портале «Женский рай» о том, что у Никиты Михалкова могут отобрать виллу в Италии, ответ получил через сутки. Для новости это не слишком оперативно, в комментариях ее бросились обсуждать тут же. Ответ гласил: «Ряд юристов отмечает, что ответственность за границу автоматически попадает под санкции. Информация о конфискации на данный момент не зафиксирована».

Проблема фейков действительно стоит остро, но нет уверенности, что ее можно решить законодательными и техническими средствами. Если пост прямо нарушает законодательство, автор должен отвечать по закону. И здесь представляется логичным подход Минцифры. Если нет – разумнее рассчитывать на

саморегулирование отрасли. На заре перестройки огромной популярностью пользовалась газета «Спид-Инфо». Помню статью «Мумия изнасиловала археолога», причем многие ей верили. Где теперь это СМИ и каков уровень доверия «желтой» прессе? По аналогичному сценарию будут развиваться и электронные СМИ, верить будут только авторитетным изданиям. Конечно, останутся сторонники «плоской Земли» и прочих экзотических и конспирологических теорий, но это будут маргинальные группы, не оказывающие существенного воздействия на общество.

Сложнее с фейками, создаваемыми в рамках информационной войны. В Великую Отечественную поступили просто – отобрали у населения радиоприемники. И некому было слушать немецкие фейки: «Сталин сдался, война проиграна».

Сегодня в лидерах по числу фейков – западные приграничные регионы: Севастополь, Крым, Белгородская область, а также Санкт-Петербург и Приморский край (рис. 5). Темы фейков становятся обстрелы и нападения диверсионных групп, подделки государственных документов об эвакуации из приграничных территорий. Все это воздействует на население, но запретами проблему не решишь. Доступ в интернет не переключишь – остается бороться, разоблачая фейки и распространяя правду. Проводить прямые репортажи с мест событий, вести открытый диалог населения с властью. Бороться правдой с постправдой. Что, конечно, гораздо сложнее. ИКС

Рис. 5. ▲ Число фейков в неделю по регионам



Технологии обмана на службе кибербезопасности

Иван Шаламов,
менеджер
продукта,
R-Vision

Риск увеличения количества и сложности кибератак сегодня достаточно высок. Справиться с ними могут помочь относительно новые для России технологии *Deception*, или киберобмана, которые создают ложные объекты ИТ-инфраструктуры, чтобы привлечь злоумышленника и заставить его себя обнаружить.

С начала текущего года количество кибератак в России увеличилось многократно. По данным «Лаборатории Касперского», только за первый квартал 2022 г. в российских компаниях произошло в четыре раза больше киберинцидентов, чем за аналогичный период прошлого года. Во многом рост числа атак на российскую инфраструктуру обусловлен обострением геополитической обстановки. События минувших месяцев заставили задуматься об информационной безопасности и государственные корпорации, и компании различных отраслей.

Под шквалом атак

С конца февраля 2022 г. хакерские группировки проводят таргетированные атаки на ключевые российские организации. Чаще всего атакуют порталы государственных органов, промышленные предприятия, ИТ- и финансовые организации. Подверглись взлому и сайты крупнейших российских СМИ.

Большая часть угроз исходит от так называемых хактивистов (хакеров-активистов). Ответственность за некоторые атаки, например на правительственные сайты, ряд СМИ и другие организации, взяла на себя хакерская группировка *Anonymous*, которая через деструктивную деятельность (взлом веб-ресурсов, выкладывание в публичный доступ или шифрование данных и т.д.) выражает свою политическую позицию.

Последствия таких атак зачастую дорого обходятся организациям: простой инфраструкту-

ры, нарушение бизнес-процессов, хищение или шифрование корпоративных данных, которые к тому же не всегда удается восстановить. Все это приводит к ощутимым финансовым потерям, наносит ущерб деятельности и репутации компании, особенно если информация о взломе попадает в средства массовой информации. А за последние несколько месяцев подобных сообщений в прессе было немало.

APT-атаки

В текущей ситуации даже у самых крупных и продвинутых компаний есть риск не справиться с хорошо спланированной целенаправленной атакой. Например, пострадал российский видеохостинг RuTube. В ночь на 9 мая видеосервис подвергся мощной APT-атаке (*Advanced Persistent Threat*, продолжительная целевая атака повышенной сложности, совершаемая организованными хакерскими группировками). Инцидент вызвал потерю доступа к платформе. Восстановительные работы продолжались трое суток. Основная сложность, по мнению технических специалистов, заключалась в восстановлении инфраструктуры, состоящей из сотни серверов. Каждый из них приходилось «поднимать» в ручном режиме. По предварительным данным, в результате атаки было поражено более 75% баз и инфраструктуры основной версии, а также 90% резервных копий и кластеров, используемых для восстановления баз данных.

APT-атаки считаются одними из самых серьезных целевых атак. При осуществлении таких атак хакеры тратят много времени на подготовку к проникновению в инфраструктуру компании, после чего закрепляются в ней, получая доступ к корпоративной сети. При этом они могут месяцами оставаться незамеченными как стандартными средствами обнаружения, так и специалистами по информационной безопасности.

Как это происходит? При проведении APT-атаки обычно используется тактика замедленного действия. Атака сильно растянута по времени, и злоумышленники, проникнув во внутреннюю сеть компании, долго ничем себя не проявляют. Это позволяет киберпреступникам максимум времени иметь доступ к необходимым им корпоративным ресурсам, оставаясь «невидимыми».

Мотивы у APT-группировок разные: от прямого хищения денежных средств, кражи персональных данных и интеллектуальной собственности до остановки деятельности конкурентов (в случае заказной атаки), нарушения работы городской инфраструктуры или попытки привлечь внимание к политической ситуации.

Как показывает практика, жертвами APT-атак становятся не только крупные компании, но и предприятия малого и среднего бизнеса. Небольшая компания может оказаться под ударом APT-атаки потому, что она обладает менее серьезной защитой.

Технологии киберобмана

Последние исследования в области кибербезопасности говорят о том, что в России риск усиления атак сегодня довольно высок. В частности, можно ожидать и новых резонансных инцидентов с участием APT-группировок. Поэтому каждой компании стоит задуматься о дополнительной защите своих информационных ресурсов.

Поиск эффективных методов защиты не так прост, ведь APT – это технически сложная кибератака. И если злоумышленнику удалось обойти средства защиты периметра организации и закрепиться в сети в обход систем защиты конечных узлов (процессов, бизнес-данных и конфиденциальных сведений, которые хранятся или передаются через устройства, подключенные к сети), то обнаружить его без специализированных систем уже практически невозможно.

Решением может стать создание дополнительного ложного слоя защиты инфраструктуры, который собьет злоумышленника с толку. Сделать это можно благодаря относительно новым для России технологиям Deception, или киберобмана.

Что такое Deception?

Deception – это централизованная система управления ложными сетевыми объектами (ловушками). Иными словами, это цифровая имитация элементов корпоративной инфраструктуры, позволяющая ввести злоумышленника в заблуждение и заставить думать, что он получил доступ к необходимым ему данным, которые на самом деле являются фэйковыми.

Системы класса Deception рассчитаны на ситуацию, когда киберпреступник уже обошел все существующие рубежи защиты инфраструктуры и находится внутри охраняемого периметра компании. Если при этом в организации не используются классические средства обнаружения и мониторинга либо они не справляются со своей задачей, то преступник остается незамеченным. И неважно, будет это опытный хакер из профессиональной группировки или же хакер-любитель, который случайно проник внутрь периметра ради собственного интереса. Deception позволит на ранних этапах обнаружить злоумышленника, замедлить его перемещение по корпоративной сети и в итоге предотвратить нанесение ущерба компании.

Технологии киберобмана используют принципиально новый подход к обнаружению вторжений хакеров, позволяя выявлять не только APT-атаки, но и атаки с использованием угроз «нулевого дня» – уязвимостей, против которых защитные меры еще не разработаны.

Как работает Deception?

Deception-платформа расставляет по реальной корпоративной сети приманки – данные, потенциально интересные для киберпреступников. Это могут быть фиктивные учетные записи пользователей, ценные корпоративные данные или «случайно» забытый файл с паролем к системе. То есть то, на что хакер с высокой степенью вероятности обратит внимание и захочет использовать для дальнейшего продвижения по инфраструктуре. Однако приманки ведут не к настоящим объектам ин-



фраструктуры, а к ловушкам – ложным узлам сети, которые имитируют реальную корпоративную систему с характерной деятельностью ее пользователей. Если в процессе разведки хакер начнет взаимодействовать с ловушкой, специалист по информационной безопасности сразу получит оповещение. При этом злоумышленник может и не догадаться, что его уже рассекретили.

Важно, что ловушки и приманки не используются в типовых рабочих процессах, а предназначены только для привлечения внимания хакеров, т.е. обычный пользователь не может случайно на них наткнуться. Поэтому любое взаимодействие с ловушкой будет свидетельствовать о том, что в корпоративной сети действует злоумышленник, который может быть не только внешним, но и внутренним. Ведь сотрудник организации тоже может попытаться завладеть корпоративными данными в корыстных интересах. Сегодня действия злоумышленников-инсайдеров – одна из основных причин утечек конфиденциальной корпоративной информации.

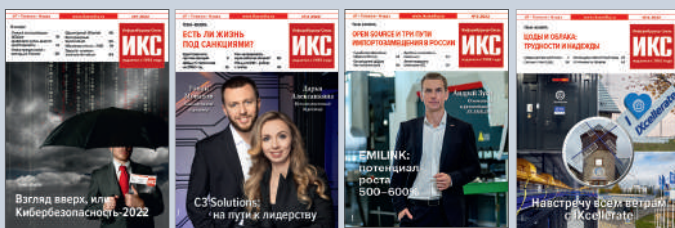
В то время как классические средства обнаружения не всегда учитывают особенности инфраструктуры компании, Desception-платформы позволяют создать ловушки и приманки, которые выглядят как единое целое с инфраструктурой. Создание реалистичных систем, не зависящих от настоящей инфраструктуры, дает возможность обнаружить активность злоумышленников раньше, чем те нанесут серьезный ущерб организации. Решения класса Desception помогут компаниям, в которых у сотрудников есть прямой доступ к высококритичным ресурсам, используются специфические активы, а также есть риск присутствия в

периметре внешнего или внутреннего нарушителя. Одно из ключевых преимуществ технологии Desception – ее незаметность для злоумышленника, а значит, само применение технологий киберобмана в корпоративной инфраструктуре скомпрометировать практически невозможно.

Курс на импортозамещение

Уход с российского рынка зарубежных производителей в области кибербезопасности поставил в уязвимое положение многие государственные и бизнес-структуры. Компании, использовавшие решения иностранных ИБ-вендоров, в том числе производителей Desception-платформ, столкнулись с серьезными киберрисками.

Российские организации уже начали переходить на отечественные продукты. Отметим, что рынок информационной безопасности в России много лет активно работал в направлении импортозамещения. Развивался и сегмент отечественных Desception-платформ. И сегодня существует ряд успешных коммерческих продуктов от российских разработчиков, которые способны заменить аналогичные системы зарубежных вендоров. Среди них есть не только единичные решения, а целые экосистемы взаимодействующих между собой продуктов, на базе которых можно построить работу центров мониторинга информационной безопасности (Security Operation Center). Такие центры мониторинга помогают экономить время благодаря автоматизации, дают возможность выявлять сложные атаки, реагировать на ИБ-инциденты, а также предоставляют инструменты, позволяющие анализировать в целом эффективность принимаемых мер. 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**



SD-WAN и безопасность корпоративных сетей



В использовании безопасных программно регулируемых зашифрованных туннелей российский рынок отстает от западного на два-три года. Освободившуюся после ухода западных компаний нишу занимают российские вендоры решений информационной безопасности.

Николай Носов

Услуги связи давно предоставляются по сервисной модели. Нет смысла тянуть свой кабель до АТС, проще ежемесячно платить оператору за телефонный номер. Цифровизация привела к необходимости передавать по сетям не только голос, но и данные. Появились дорогие выделенные линии, связывающие разбросанные по стране подразделения компаний. Телеком-операторы устанавливают на них свои маршрутизаторы и сдают каналы в аренду. Сильно удешевил связь интернет. Однако соединение через публичный интернет нельзя назвать безопасным. Компании начали создавать поверх интернета частные виртуальные сети (Virtual Private Network, VPN), а операторы – предоставлять как услугу свои, более надежные VPN-каналы.

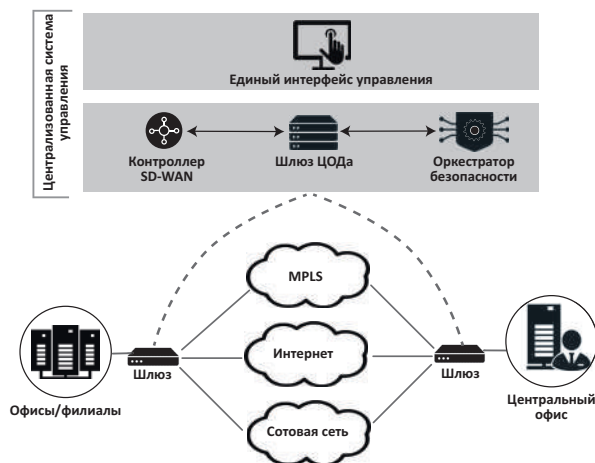
С распространением облачных сервисов компаниям понадобилось связываться по внешним сетям не только со своими подразделениями и дата-центрами, но и с площадками облачных провайдеров. Еще сильнее размыла периметр безопасности компаний эпидемия COVID-19. Массовый переход на удаленную работу потребовал обеспечения надежной и безопасной связи сотрудников с информационными системами предприятий из разных мест и с самых разных устройств. На помощь опять пришли операторы связи, предлагая безопасную сеть по сервисной модели. На Западе даже появился термин «сеть как услуга» (Network as a Service, NaaS).

Надежность связи обеспечивается резервированием каналов, причем самых разных – от выделенных линий и MPLS до мобильной и спутниковой связи и интернета. Вручную сетевикам переключать проблемные каналы сложно, балансировать нагрузку, оптимизировать трафик, почти невозможно. Для решения этих задач начали использовать технологию программно определяемой территориально распределенной сети (SD-WAN), которая позволяет создавать программно управляемые зашифрованные оверлейные туннели поверх существующих сетей. Благодаря шифрованию каналы связи защищены.

За рубежом технология активно внедряется с 2018 г. и на кривой Gartner уже выходит на плато продуктивности. В мировых лидерах – компании Fortinet, VMware и Cisco (все они на сегодня работу на российском рынке прекратили).

NaaS и SD-WAN

SD-WAN – это применение идеологии программно определяемых сетей к распределенным корпоративным сетям. Идея та же – отделение уровня управления процессом передачи данных (Control Plane) от собственно уровня передачи (Data Plane), что позволяет гибко и централизованно управлять сетями, получать «управляемый VPN», да еще и с дополнительными полезными опциями, такими как балансировка нагрузки по всем имеющимся каналам.



Архитектура SD-WAN

На площадках распределенной корпоративной сети устанавливаются оконечные устройства, к внешним портам которых подключаются различные каналы связи: интернет, сеть MPLS, сотовая сеть (см. рисунок). Оконечное устройство имеет WAN-порты, отличающиеся от обычных сетевых портов поддержкой функций SD-WAN. Первая из таких функций – автоматическая настройка криптографически защищенных туннелей. Вторая – интеллектуаль-



Алексей Кудрявцев, руководитель управления сетевых решений кибербезопасности, Bi.Zone

Большинство компаний, которые пользуются NaaS операторов связи, постепенно перейдут на услуги на платформе SD-WAN. Для операторов и компаний это намного удобнее. Если раньше заказчику нужно было разворачивать традиционные сетевые решения и иметь многочисленный персонал для их обслуживания, то с SD-WAN таких сотрудников требуется меньше за счет централизованного управления.

ное переключение трафика между этими туннелями. Переключение осуществляется не только в случае выхода канала из строя, но и при ухудшении качества связи, задержки или уровня потерь пакетов. Например, если первый канал перегружен, то передача голоса переключается на другой. Это один из самых частых вариантов. Также каналы можно агрегировать. Скажем, если банкомат имеет доступ к двум каналам связи, то можно один разгрузить и обеспечить балансировку. Централизованная система управления (уровень Control Plane), включающая шлюз дата-центра, контроллер SD-WAN и оркестратор безопасности, находится в центральном офисе (в случае модели on-premise) или у оператора связи (в случае модели MSP).

Удобство централизованного управления программно определяемыми распределенными сетями быстро оценили операторы связи, предлагающие услуги NaaS. Действительно, не нужно привлекать специалистов по настройке сетей: на удаленных площадках достаточно подсоединить оконечное устройство к сети, включить питание, нажать на ссылку активации, и за 15 минут будет создано подключение к сети оператора связи, у которого уже установлен центральный контроллер. Клиент получит учетную запись и сможет управлять своими VPN-каналами.

SD-WAN в России

На российском рынке пионером SD-WAN стала МТС, начавшая в 2020 г. использовать решения Fortinet. Во многом благодаря совместным проектам вендора и оператора российский рынок услуг SD-WAN в 2021 г. достиг 1,45 млрд руб. (данные iKS-Consulting). Свой вклад в популяризацию технологии внесла компания Bi.Zone, выпустившая в 2021 г. первое отечественное решение SD-WAN.

Решения SD-WAN можно рассматривать как подмножество более широкого класса систем

VPN. Причем в 2021 г. их доля на западном рынке превысила долю традиционных VPN-решений. Учитывая наше отставание, которое эксперты оценивают в два-три года, можно ожидать, что в России доля решений SD-WAN на рынке VPN превысит 50% в 2023–24 гг. В деньгах оценить сложнее: объем рынка VPN в целом, который в 2021 г., по данным iKS-Consulting, составил 44,53 млрд руб., в 2022 г., как прогнозирует консалтинговое агентство, из-за санкций уменьшится на 3,4%. Дальнейшие изменения ввиду высокой турбулентности в геополитике предсказать трудно. Но если спад удастся остановить, объем российского рынка SD-WAN в 2023–24 гг. составит примерно 22 млрд руб.

Санкции и уход зарубежных вендоров приведут к распределению рынка между российскими игроками. На решения open source рассчитывать трудно – первый и единственный продукт с открытым кодом FlexiWAN имеет крайне ограниченный функционал и по сути является централизованно управляемым традиционным маршрутизатором, в котором от SD-WAN нет почти ничего. Остаются российские решения: Bi.Zone Secure SD-WAN и вышедшее на рынок в 2022 г. Kaspersky SD-WAN. Скорее всего, между ними и развернется конкурентная борьба за клиентов, у которых будут заканчиваться лицензии зарубежных вендоров, и за новых заказчиков, решивших развернуть или модернизировать корпоративные сети. Наиболее вероятными пользователями услуг NaaS станут компании среднего и малого бизнеса, имеющие более десятка удаленных площадок.

Оба российских вендора специализируются на безопасности, и именно необходимость защиты распределенной корпоративной сети, создания решений для находящейся сейчас на вершине хайпа технологии безопасного пограничного доступа (SASE) побудила их заняться SD-WAN. Ведь модель SASE включает помимо служб сетевой безопасности, таких как межсетевой экран (МСЭ) следующего поколения, безопасный веб-шлюз, сетевой доступ к сети с нулевым доверием, посреднические службы облачной безопасности и SD-WAN. И решения SD-WAN необходимы для обеспечения комплексной безопасности корпоративных сетей клиентов.

Впрочем, спектр отечественных решений SD-WAN не ограничивается двумя вышеперечисленными. В реестре российского ПО зарегистрирована система «Богатка» на основе технологий программно определяемых сетей от московского производителя сетевого оборудования Network Systems Group. Но в информационном поле компания активности не проявляет, сведений о внедрениях нет, и оценить потенциал решения сложно.

Спрос большой, но есть проблемы с функциональностью

После 24 февраля минувшего года, как сообщил Алексей Кудрявцев, руководитель управления сетевых решений кибербезопасности компании Bi.Zone, число запросов от клиентов, интересующихся Bi.Zone Secure SD-WAN, возросло более чем в 20 раз. Причем одним клиентам достаточно сетевого решения класса SD-WAN со стандартным МСЭ L4, и существующий продукт Bi.Zone их полностью удовлетворяет. У других организаций, применявших ранее системы зарубежных вендоров, есть сложившийся набор требований. Например, многим нужны динамические протоколы маршрутизации. Большинству подходит имеющийся в решении протокол BGP, но некоторым нужен OSPF, который пока не поддерживается. Возникают требования к кластеризации, к распознаванию приложений. У ряда западных вендоров есть MPLS VPN «из коробки», но в российских решениях для корпоративного рынка полноценный промышленный MPLS VPN в настоящий момент отсутствует.

Серьезные требования выдвигаются к МСЭ. Для соответствия SASE многим заказчикам на оконечных устройствах (Bi.Zone CyberEdge) нужны межсетевые экраны нового поколения, анализирующие трафик не только по адресам и портам, но и по сигнатурам. Эту функциональность Bi.Zone собирается реализовать в I квартале 2023 г. Несмотря на то что сегодня решение российского разработчика не обладает всем спектром функциональных возможностей зарубежных аналогов, для конкретного заказчика может быть установлен срок, в течение которого он получит требуемую ему функциональность. По словам А. Кудрявцева, доработка обычно занимает один-два квартала.

Для доступа к облакам в дата-центрах размещаются виртуальные машины, подключающиеся к нужным сервисам. Bi.Zone Secure SD-WAN поддерживает стандартные гипервизоры VMware и Qemu/KVM, но есть и нестандартные облака, как правило, это сложные кастомизации OpenStack. Пока решение поддерживает только облако Cloud (ранее SberCloud). Среди нестандартных проблем других облаков – невозможность в автоматическом режиме создать виртуальную машину с двумя сетевыми интерфейсами. Например, в Yandex.Cloud для этого нужно создавать заявку в службе поддержки облака.

Пользователи SD-WAN

Основное направление развития NaaS – привлечение средних и малых предприятий. Чем меньше бизнес – тем выгоднее использовать аренду, в случае SD-WAN – совместно использо-

Для нас малый бизнес – это большой бизнес. Мы понимаем, что основные триггеры для выбора решений SD-WAN у компаний малого и среднего бизнеса – это простота и удобство работы.

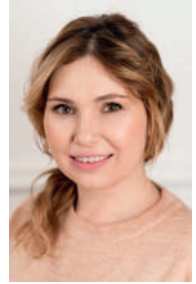
Концепция SD-WAN подразумевает максимальное упрощение и автоматизацию работы с сетевым оборудованием, что оценят небольшие компании, в которых нет выделенного ИТ-отдела, но есть множество филиалов и/или идет активное развитие.

вать ресурсоемкий центральный контроллер оператора. Крупные заказчики, вероятнее всего, захотят иметь собственный централизованный контроллер, но в условиях санкций и дефицита оборудования могут выбрать облачную модель.

Как показал анализ рынка, пользователи, уже внедрившие или пилотирующие решения SD-WAN, работают в самых разных отраслях. Чаще всего это банки и финансовые организации, промышленные предприятия, энергетики, телеком-операторы, строительные компании. Бюджетным организациям и госструктурам интересно использовать решения по модели NaaS. Это справедливо и для предприятий из системы образования. Между моделями NaaS и on-premise выбирают клиенты из ритейла, медицины, фармацевтики, ЖКХ и ИТ-компании.

У каждого пользователя свой тип трафика. Например, трафик банкомата существенно отличается от трафика школы. В школах требуется защита от атак изнутри – там важно иметь набор систем безопасности непосредственно на площадке. Зато там есть администраторы, которые могут перенастраивать оконечное устройство. А вот банкоматы перенастраиваются крайне редко и защищаются централизованно. Они не взаимодействуют друг с другом, объем трафика мал, поэтому для них требуется простое устройство с минимальными производительностью и ценой.

«К концу 2022 г. мы внедрим свое решение на сотнях площадок. У наших партнеров, которые строят решения NaaS, уже есть очередь из клиентов, желающих подключиться через SD-WAN. Один из крупных операторов планирует в следующем году подключить не менее тысячи новых SD-WAN устройств», – делился планами А. Кудрявцев. Заказчики начинают доверять управление корпоративными сетями передачи данных операторам связи и видят в использовании NaaS с SD-WAN экономическую выгоду. ИКС



Анна Комша,
руководитель
направления
развития сетевой
безопасности,
«Лаборатория
Касперского»

Интеллектуальные блоки розеток с измерительным модулем

Производственная группа REMER пополнила ассортимент интеллектуальных PDU моделями собственной разработки с измерительным модулем MI.



Новые PDU в режиме реального времени обеспечивают измерение параметров питания по каждой фазе и контуру с погрешностью не более 1%. PDU оснащены OLED-дисплеем, на котором отображаются значения напряжения, тока и мощности, информация о нагрузках по каждому контуру или фазе, состояние датчиков и внешних устройств, сетевые настройки – IP- и MAC-адреса, модель, серийный номер и версия ПО. Меню дисплея имеет интуитивно понятную четко структурированную концепцию управления.

Дистанционная настройка и мониторинг доступны через русскоязычный веб-интерфейс, интерфейс командной строки (CLI) или протокол управления сетью (SNMP).

PDU с контроллером и измерительным модулем оснащены шнуром питания необходимого сечения и соответствующей вилкой стандарта IEC 60309, а для визуального разграничения и удобства распределения нагрузки розеточные выходы каждого контура или фазы выделяются цветом. Благодаря универсальной системе безинструментального монтажа установка PDU REM возможна как на вертикальные органайзеры, так и на вертикальные юнитовые направляющие напольных шкафов.

Характеристики PDU с контроллером и измерительным модулем:

- интерфейс Ethernet 10/100BASE-TX как основной канал связи с устройством;
- настройка, управление и мониторинг по протоколам SNMP v1/v2c/v3, Telnet и Web или посредством USB-порта Type-C;

- поддержка протокола TFTP для обновления ПО, импорта или экспорта конфигурации;
- настройка NTP, SMTP, Watchdog;
- подключение до 10 датчиков 1-Wire;
- подключение внешних датчиков и приборов охранно-пожарной сигнализации в 6/12 дискретных входов/выходов и в 2/4 аналоговых входа;
- подключение цифровых устройств с интерфейсами RS-232, RS-485;
- применение встроенного сигнального реле для подключения сирены;
- настройка подключенных устройств по протоколу Modbus;
- мониторинг напряжения, тока и мощности по каждой фазе или группе розеток;
- мониторинг состояния дискретных и аналоговых входов;
- хранение аварийных сообщений и передача их в систему мониторинга;
- время наработки на отказ более 200 000 ч;
- автономная работа встроенных часов реального времени при отключении питания в течение 7 дней.

www.cmo.ru

Линейка онлайн-ИБП

Компания «Металлоизделия и комплектующие» начала производство источников бесперебойного питания. Линейка продукции включает в себя однофазные и трехфазные, стоечные и напольные онлайн-ИБП мощностью от 800 Вт до 36 кВт.



ИБП МиК совместимы с любыми типами нагрузок и поддерживают возможность параллельной установки. Для увеличения срока службы батарей предусмотрено управление током заряда. Реализована полная защита от перенапряжений, коротких замыканий и перегрева; скорость вращения вентиляторов изменяется автоматически, что обеспечивает адекватный уровень шума в помещениях с ИБП.

ИБП МиК оснащены ЖК-дисплеем и светодиодной индикацией, а также внешними интерфейсами RS-232 и USB. Также предусмотрена установка карты расширения SNMP, благодаря чему возможны постоянный мониторинг состояния устройств и включение их в сетевую инфраструктуру.

metalkomp.ru

ЦОДЫ, ОФИСЫ, ОБЩЕСТВЕННЫЕ ПРОСТРАНСТВА

11 апреля 2023 ⇌ Москва



СТРУКТУРИРОВАННЫЕ
КАБЕЛЬНЫЕ
СИСТЕМЫ



Реклама / 16+

Конференция для профессионалов, занимающихся проектированием, построением и эксплуатацией кабельных систем ЦОДов, офисных центров, объектов общественного пространства (ТРЦ, стадионы, выставочные комплексы, транспортные узлы, парковые зоны и пр.).

Основная задача конференции СКС-2023 – обмен знаниями и наилучшим опытом в области проектирования, построения и эксплуатации кабельных систем. Предполагается рассмотреть основные тенденции в области СКС, новые технологии и технические решения, актуальные вопросы выбора продуктов.

В фокусе форума СКС-2023:

- ↳ Российский рынок СКС. Карта вендоров
- ↳ Основные технологические тенденции в области СКС
- ↳ Управление и автоматизация
- ↳ Выбор поставщика СКС в новых реалиях

При поддержке

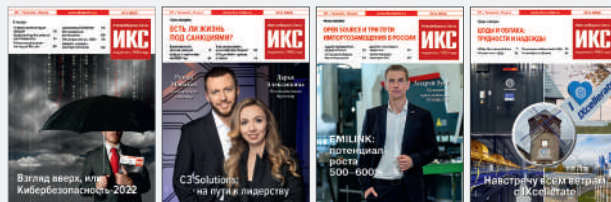


cable.iksmedia.ru

КОЛОНКА РЕДАКТОРА / № 1-4



- 5G как сервис, или Облака опускаются на землю . . . № 1
- Инженерка будет! № 2
- Моновендорные ЦОДы: быть или не быть? № 3
- Восходящий рынок Центральной Азии. № 4



ИКС-ПАНОРАМА / № 1-4



- Быть ли уральской агломерации ЦОДов? . . № 1**
- ИТ в медицине: от информатизации к цифровой трансформации № 1
- АНО КС ЦОД: учимся эксплуатации № 1
- Цифровизация медицины для увеличения продолжительности жизни № 1
- Региональные ЦОДы – лучший объект для инвестиций № 2**

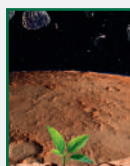


- За облаками, как за сахаром в «Пятерочке» . . № 2
- Криптовалюта против санкций № 2
- С оптимизмом из Питера № 3**
- DCDE-2022: надо ловить волну № 3
- Рынок ЦОДов: рост на фоне спада № 4**
- Готовы к рывку № 4
- Казахстан задает цифровую моду № 4
- Дайджест отрасли ЦОДов № 1-4**

ЭКОНОМИКА И БИЗНЕС / № 1-4



- Н. Носов. Цифровой рубль вместо криптовалюты и другие блокчейн-итоги 2021 года № 1**
- А. Эрлих. Пандемия и цодостроение. Опыт Германии № 1
- А. Столяров. Эксабайты данных и всевластие мессенджеров: тренды и вызовы для телекома. № 1
- Ю. Христова. Найти и удержать: как изменились ожидания кандидатов в ИТ-сфере № 1



- Т. Толмачева. Есть ли жизнь под санкциями? № 2**
- О. Киселев. Ждать не стоит импортозамещать № 2
- А. Казённов. «Бес» паники: технологии у нас есть. № 2
- Н. Носов. Время делать самим № 2
- Н. Носов. Утечка мозгов и господдержка отрасли № 2
- Е. Вирцер, А. Мартынюк. ЦОДы в регионах: предложение рождает спрос № 2
- И. Бакланов. Новое Средневековье № 2



- И. Остаполец. Как создавать системы электроснабжения ЦОДов сегодня № 3**
- Р. Шамаков: «Успеха добьются те, кто придерживается системного подхода» . . . № 3
- Н. Носов. Либерализация реестра российского ПО: за и против № 3
- С. Бочкарев: «Нам важно увеличить темпы строительства» № 3
- Т. Толмачева. Появятся ли на российской периферии периферийные ЦОДы? № 3
- Дж. Гуо, Т. Шабаев. ТИСА претендует на лидерство № 3



- И. Бакланов. О дивный старый мир! № 4**
- Н. Носов. Цифровой рубль становится ближе № 4
- К. Чеханков. ИТ-трансформация бизнеса: выстраиваем процесс правильно. № 4
- А. Барсков. ГИСы уйдут в коммерческие ЦОДы № 4

ИНФРАСТРУКТУРА / № 1-4

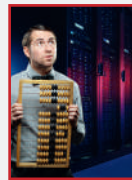


- Н. Носов. Гонка процессоров – взгляд из России. № 1**
- А. Хашимов. В трети проектов альтернативы литий-ионным АКБ нет. № 1
- С. Бочаров. МЕС в ожидании 5G № 1
- Н. Ефимов. Высокие скорости в ЦОДах: поддержка будущих потребностей. № 1
- А. Ежов. Кондиционеры LCP CW для охлаждения высоконагруженных стоек и суперкомпьютеров № 1
- А. Семенов. Однопарный Ethernet № 1



- М. Саликов. «Хайтед»: новая команда на рынке цодостроения № 1
- И. Малахов. Аналоговые приборы учета: модернизировать или менять на цифровые? . № 1
- А. Зуев. Три специализированные роли рядного шкафа в ЦОДе № 1
- А. Ходырев. Связанные одной сетью: какой способ подключения к облаку выбрать? № 1
- А. Бутенко. Conteg – это европейская этика производства № 1
- Э. Лоуренс, Р. Асьерто, Д. Бизо, Т. Рахконен. Пять прогнозов развития ЦОДов на 2022 год. № 2**

- Д. Алексанкина, Р. Монахов. C3 Solutions: на пути к лидерству № 2
- Д. Бизо. Новые рекомендации ASHRAE – вызов энергоэффективности № 2
- В. Гавричков. KeHua в России: режим работы – штатный, рост – трехкратный № 2
- А. Жумыкин. Легенды и мифы датацентров . . . № 2
- Когда глобализация больше не работает № 2
- О. Нечай. Автоматизация и роботизация в дата-центрах: время пришло № 2
- Г. Бабаевский. Eurolan: время быстрого роста № 2
- О. Нечай. Облака-2022: устойчивость на всех уровнях № 2
- А. Семенов. Технология PoLAN построения локальных сетей. № 2
- А. Можяев. Шинопроводы мирового уровня – для российских дата-центров. № 2
- А. Барсков. Охлаждение для ЦОДа: обойдемся без компрессоров? № 3**
- Е. Вирцер, А. Мартынюк. Key Point: 35 дата-центров за пять лет! № 3
- Н. Носов. Инженерная переключка. № 3
- EMILINK: потенциал роста 500–600% № 3
- И. Кузнецов. Дробим «инженерку» правильно. . . № 3
- Л. Юль. Все для ЦОДа от C3 Solutions. № 3



- Н. Носов. Квартиры для серверов № 3
- А. Семенов. Зачем повышать категорию СКС . . . № 3
- Российское DWDM-решение для межсоединений ЦОД № 3
- О. Нечай. Частные сети 5G: пора не пора – иду со двора № 3
- А. Павлов. От чего зависит стоимость проектирования и строительства ЦОДа? . . № 4**
- С. Вышемирский. Как строить ЦОДы в условиях санкций № 4
- Г. Юдин, А. Кузнецова. Выбор оптимальной концепции охлаждения майнингового ЦОДа. . № 4
- Д. Бизо, Л. Саймон, Ж. Дэвис. Прямое жидкостное охлаждение: переход неизбежен. № 4
- А. Соловьев. Трансформация бизнеса, трансформация продуктового предложения. . № 4
- А. Семенов. Архитектура Spine – Leaf в ЦОДах: зачем нужна и как реализовать № 4
- Н. Куликов. Wi-Fi на 6 ГГц. Куда все идет? . . . № 4
- А. Яковлев. «Мы ориентируемся на стандарты качества мировых лидеров СКС». № 4
- Н. Носов. Удаленный доступ через VPN в новой реальности. № 4
- А. Зуев. EMILINK: собственное производство = оптимальная цена + контроль качества № 4

СЕРВИСЫ И ПРИЛОЖЕНИЯ / № 1-4



- Н. Носов. ИИ художник и поэт № 1**
- Н. Носов. Бессерверные вычисления вчера, сегодня, завтра № 1
- А. Салов. Облачные итоги – 2021 № 1
- С. Мирин, Д. Патрикеев. Облака-2021: ковидное ускорение. № 1
- Е. Макарыин. Выбор облачного провайдера в РФ: взгляд клиента № 1



- А. Салов. Облачные тренды – 2022 и взгляд в будущее № 2**
- Я. Камыс. Как мигрировать в российские облака? 10 рекомендаций № 2
- Е. Галкин. Инфраструктура открытых ключей в здравоохранении № 2

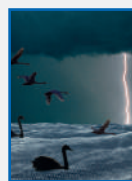


- Д. Лившин. Нейросети и машинное обучение в девелопменте: от «умных» камер до виртуальных дворцовых. № 2
- Н. Носов. Open source и три пути импортозамещения в России № 3**
- Н. Носов. Каким будет «суверенный GitHub»? . . № 3
- С. Кикило. «Суверенный GitHub» – хорошее решение № 3
- Н. Носов. ЦОДы и облака: трудности и надежды № 4**
- О. Роджерс. Основные принципы масштабируемости и устойчивости облаков . . № 4
- Н. Носов. Многоквартирное жилье становится умнее № 4
- А. Новак. Искусственный интеллект в видеоаналитике. Реальные возможности . . № 4

БЕЗОПАСНОСТЬ / № 1-4



- Н. Носов. Взгляд вверх, или Кибербезопасность-2022. № 1**
- С. Сенютин. Защита ИСУ электроэнергетики: не опоздать и правильно построить № 1
- Н. Носов. КИИ: враг внутри № 1
- Н. Носов. Кибервойна: острая фаза № 2**
- Н. Носов. ПО для КИИ – рубим с плеча. № 2



- Н. Носов. Каждой компании – своего киберкомиссара № 3**
- Д. Кузнецов. Безопасников понадобится больше № 3
- Н. Носов. Шпаргалки для киберкомиссаров. . № 4**
- Н. Носов. Остановить телефонных мошенников № 4
- НОВЫЕ ПРОДУКТЫ № 1-4**

ДИ СИ КВАДРАТ

Тел.: (495) 776-8883
E-mail: pm@dcxdc.ru
https://dcxdc.ru/..... 1-я обл., с. 16–17

СВОБОДНЫЕ ТЕХНОЛОГИИ

ИНЖИНИРИНГ
Тел.: (495) 120-2866
E-mail: info@sv-tech.ru
www.sv-tech.ru..... с. 9

СПЕЦИАЛИЗИРОВАННЫЕ КАБЕЛЬНЫЕ

СИСТЕМЫ
Тел.: (495) 721-8852
E-mail: info@cablingsystems.ru
https://cablingsystems.ru/.... с. 34–35

#CloudMTS

Тел.: (800) 250-1001
E-mail: support@cloud.mts.ru
https://cloud.mts.ru/..... с. 32–33

EMILINK GROUP

Тел.: (800) 777-1300
E-mail: info@emilink.ru
www.emilink.ru..... с. 48–49

HYPERLINE

Тел.: (800) 555-0660
E-mail: info@hyperline.ru
www.hyperline.ru..... с. 54–55

KEY POINT

Тел.: (800) 600-3557
E-mail: info@dc-keypoint.ru
www.dc-keypoint.ru.. с. 18–19, 4-я обл.

SYSTEME ELECTRIC

Тел.: (495) 777-9990
e-mail: ru.ccc@se.com
www.systeme.ru..... 2-я обл.

Указатель фирм и организаций

3M	53	Ofcom	15	«ВымпелКом»	5	«РЕД СОФТ»	24, 25
360tv	68	Oracle	22	Высшая школа экономики	68	РЖД	28, 55
Alibaba	29	OrbitsEdge	37, 38	ВЭБ.РФ	18, 19	«Рокитсофт»	27
Amazon	15	Oxygen	5, 6	Газпромбанк	28	НТЦ ИТ РОСА	25, 26
Amazon Web Services	13, 29, 36	Panduit	1, 51	«Газпром трансгаз»	28	«Росатом»	28
Antarctis	7	Red Hat	22, 25, 26	НПП «Гиперлайн»	54, 55	Росгвардия	58
Axoft	30	Rogue Space Systems	38	«Голден Телеком»	16	Росгеология	28
C3 Solutions	7	RuTube	70	«ДАКОМ М»	25	Роскомнадзор	68
Capella Space	36	R-Vision	70	«Датарк»	7	«Роскосмос»	38, 39
CipherCloud	31	Selectel	27, 29, 31	АНО «Диалог»	67	«Росплатформа»	26
Citrix	22	Senko	51, 53	АНО «Диалог Регионы»	67, 68, 69	Роспотребнадзор	28
Cloud	8	Serverspace	26, 29	«Ди Си Квадрат»	5, 16, 17	«Ростелеком»	28, 30
Cloud4y	28, 29	SES	36	ДИТ Москвы	28	«Ростелеком-ЦОД»	5
CommScope	1	Skype	61	«ИКС-Медиа»	4, 16, 29	«Ростех»	28
CommuniGate Systems	61	ГК Softline	6, 8, 60, 63	«Информационные спутниковые системы им. акад. М.Ф. Решетнёва»	40	«Росэнергоатом»	28
Corning	1	SpaceX	36	«ИСПсистем»	25	«РусБИТех-Астра»	24, 25, 27, 28
The Daily Telegraph	69	Stackalytics	29	НПП «Исток»	28	«Руссофт»	30, 31
DATALAN	35	Stack Group	16, 28, 29	«ИТ-Град»	26	«Рустэк»	25, 27, 28, 29, 30, 31
DataLine	5	Step Logic	41	«Казахтелеком»	8	Сбербанк	29, 30
Delta	41, 42, 44, 45, 46	Sumitomo Electric	52	«Казтелепорт»	8	«СберЗдоровье»	59
Digital Energy	30	Sun	22	КНС Групп	28	«Сбертех»	27, 30
Emilink	6, 7, 48, 49	Symantec	31	АНО «Координационный совет по ЦОДам и облачным технологиям»	8	«СБКлауд»	28, 29
Euromicron	53	T1	30	Корпорация развития Дальнего Востока и Арктики	18, 19	«Свободные Технологии Инжиниринг»	6
Forcepoint	31	Telegram	67	КРОК	27, 28, 30, 31	«Сервионика»	29
Google	15	Treolan	30	«КРОК регионы»	27	«Скала Софтвр»	30
Google Cloud	36	TÜV Austria	8	«Лаборатория Касперского»	70	Совет по стратегическому развитию и национальным проектам	58
GreenBushDC	32, 33	Uptime Institute	8, 10, 11, 12, 14, 17, 18, 32	«Марвел-Дистрибуция»	30	«СофтЛайн Платформы»	25
Hewlett Packard Enterprise	39	USC	37, 39	НИИ «Масштаб»	25	ТАСС	68
Huawei	29	US Conec	51	МВД	58	«Технологии Доверия»	8
Hyperline	55	US ElectroDynamics	36	«МегаФон»	5	«Техносерв»	30
iKS-Consulting	4, 8, 43	Vector	37	Минздрав России	57, 58	«Тионикс»	27, 30
Intuitive Machines	39	Viasat	36	Министрство цифрового развития, инноваций и аэро- космической промышленности Республики Казахстан	8	ТНК-ВР	16
ISPsystem	31	VK	29, 31, 61	Минтруд России	28	Управление Президента РФ по развитию информационно- коммуникационных технологий и инфраструктуры связи	68
ITglobal.com	26, 27, 28	VK Cloud	29, 30	Минцифры России	8, 21, 24, 27, 28, 30, 31, 60, 68, 69	УЦСБ	6, 7
IXcellerate	8	VMware	22, 23, 25, 26, 27, 29, 30, 31, 63	Минцифры Челябинской обл.	28	Федеральная кадастровая палата	28
Kehua Tech	7, 41, 42, 44, 45, 46	WS Aerospace & Satellite Solutions	36	НИАУ МИФИ	28	ФНС	28
Key Point	5, 8, 17, 18, 19	Yandex Cloud	29	ГБ МСЭ по Еврейской АО	28	Фонд развития цифровой экономики	57
Key Point Group	5, 18	Zoom	61	МТС	26, 32, 33	Фонд социального страхования	28
KSAT	36	ГК «Айтеко»	29	МТУСИ	50	ФСТЭК	31
Lattelecom	28	«Айтеко Cloud»	28, 29	НИКИЭТ	28	ГК «Хост»	25
Legrand	53	ГК «Астра»	24, 25, 27, 28, 31, 60, 62	ГК НКТ	35	Центризибирком	28
Lenta.ru	68	АСВ	28	«Облачная платформа»	28, 30	ГАУ СО ЦТЗ	28
Lockheed Martin	37	Ассоциация участников рынка спутниковой связи	40	«Одноклассники»	67	«Шаркс Датацентр»	25
Loft Orbital	37	НИЦ «Аэродиск»	26	«Орион»	25	ГХ «Электросистемы»	7
Lonestar Data Holdings	39	«Базальт СПО»	24, 25	«Парус электро»	7	«Юкос»	16
Mail.ru	29	«Базис»	25, 27, 28, 30, 31	Почта России	28	«Яндекс»	27, 29, 31
Mail.ru Cloud Solutions	30	ИЦ «Баррикады»	25	Правительство Москвы	57		
Makecloud.ru	28	«Велвика»	25				
ГК Merlion	30	«ВКонтакте»	67				
MerlionCloud	28, 29	«ВК Цифровые технологии»	27				
Microsoft	13, 15, 22, 29, 31, 36, 39, 61	ВТБ	16, 27, 29, 30				
Mont	30						
NASA	39						
Nutanix	26						
NVIDIA	37						

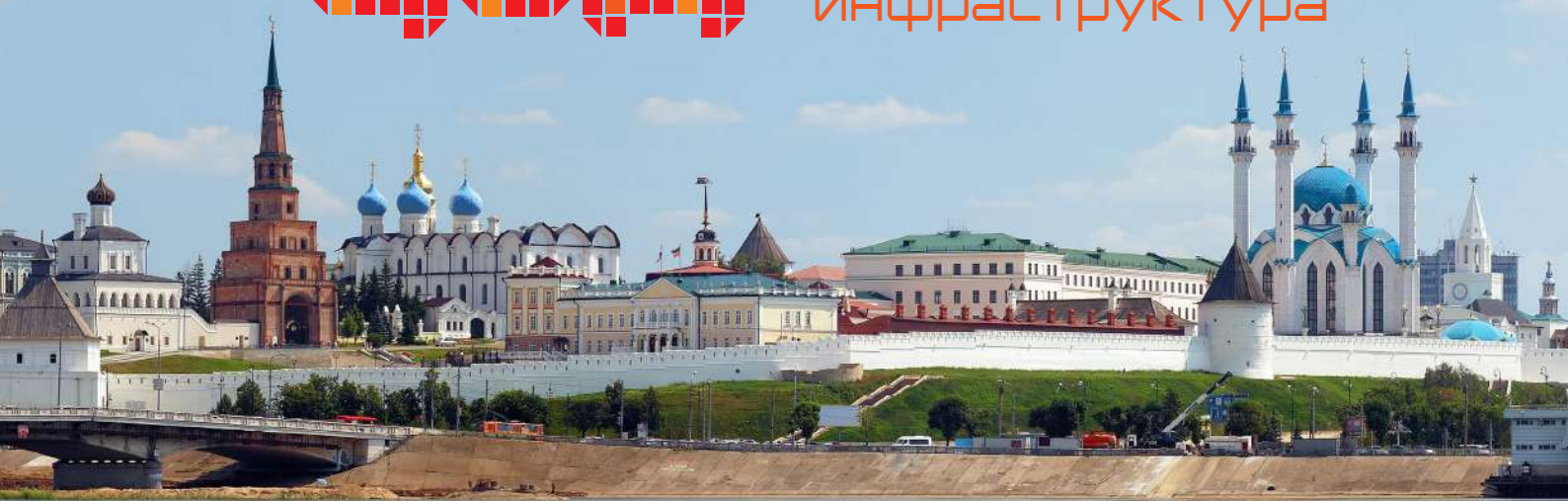
Учредитель журнала «ИнформКурьер-Связь»:

ООО «ИКС-МЕДИА»:

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



МОДЕЛИ
сервисы
инфраструктура



Казань
Korston Royal Kazan

КОНФЕРЕНЦИЯ И ВЫСТАВКА 20 апреля 2023

Конференция «ЦОД: модели, сервисы, инфраструктура» в Казани – представительная площадка для обсуждения актуальных вопросов индустрии дата-центров в Татарстане и Приволжском федеральном округе в целом. В фокусе конференции – экономические, организационные и технические вопросы, связанные с развитием ЦОДов и предоставляемых на их базе услуг, в том числе облачных сервисов.

Фокус конференции

- Экономика и бизнес-модели региональных ЦОДов
- Модульные, контейнерные и prefab-ЦОДы
- Облачные сервисы для региональных потребителей
- ЦОД как элемент распределенной системы отказоустойчивости
- ИТ-инфраструктура ЦОДов

подробно о программе
и участниках
на сайте конференции



Реклама

16+

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

ОРГАНИЗАТОРЫ



ПРИ
ПОДДЕРЖКЕ
И УЧАСТИИ



КООРДИНАЦИОННЫЙ СОВЕТ
ПО ЦОДАМ И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ
Автономная некоммерческая организация

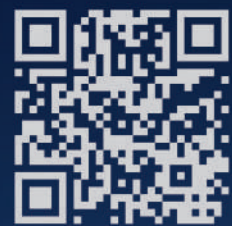


KEY POINT GROUP

РЕГИОНАЛЬНАЯ СЕТЬ ЦОД ВАЖЕН КАЖДЫЙ!



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



keypoint-group.ru