ТЕМА НОМЕРА

ИТ-ИНФРАСТРУКТУРА ДЛЯ ИИ

ИнформКурьер-Связь
ИКС
издается с 1992 года

МЕРОПРИЯТИЯ ИКС-МЕДИА

ИКС

2025

- Data Center Design & Engineering Kazakhstan 18.02
- CLOUD & CONNECTIVITY 18.03
- СКС. ЦОДы, офисы, общественные пространства 02.04
- ЦОД: модели, сервисы, инфраструктура 16.04/17.06/25.11
- Data Center Design & Engineering 20.05
- DC AWARDS 17.06
- ЦОД 2025 03–04.09
- Data Center & Cloud Kazakhstan 07.10
- Eurasia Data Center & Cloud Forum 04.11

Реклама/16+

География:
Москва
Санкт-Петербург
Екатеринбург
Новосибирск
Ташкент
Алматы

подробнее
на сайте iksmedia.ru

Издается с мая 1992 г.

Издатель
ООО «ИКС-МЕДИА»

участник
АНО КС ЦОД

КООРДИНАЦИОННЫЙ СОВЕТ ПО ЦОДам И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ
Автономная некоммерческая организация

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

Учредитель:
ООО «ИКС-МЕДИА»

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

РЕДАКЦИЯ
iks@iksmedia.ru

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

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

Корректор
Е.А. Краснушкина

Дизайн и верстка
Е.В. Денисова

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

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

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

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

Дата подписания в печать: 01.11.24.
Дата выхода в свет: 12.11.24.
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

12+

ИИ как цифровой МММ?

В то время как российские аналитики соревнуются, кто напророчит большее влияние искусственного интеллекта (ИИ) на будущее российской экономики, в США нарастает скепсис относительно перспектив этой технологии. Все чаще говорят о том, что ИИ (если оперировать любимыми американцами терминами Gartner) скатывается в «пропасть разочарований» и непонятно, в каком виде он выйдет на «плато продуктивности».

По оценкам Goldman Sachs, в ближайшие годы крупные технологические корпорации потратят на обеспечение поддержки ИИ около $1 трлн. Это четверть федерального бюджета США. Но все больше инвестиционных банкиров высказывают опасения в способности big tech превратить технологию в прибыльный бизнес. Другими словами, просто не верят, что эти инвестиции окупятся.

Аналитики Barclays прогнозируют, что инвесторы будут вкладывать ежегодно $60 млрд только в разработку моделей ИИ. Этого достаточно для создания 12 тыс. продуктов, сопоставимых по производительности с ChatGPT. Но нужно ли миру столько подобных систем?

По недавно опубликованным данным Бюро переписи населения США (United States Census Bureau), только 5,1% американских компаний используют искусственный интеллект для производства товаров и услуг, тогда как в начале 2024 г. этот показатель составлял 5,4%.

А вот цифры «ближе к ЦОДам»: согласно опросам Uptime Institute, в 2022 г. 76% руководителей и менеджеров ЦОДов были готовы доверить ИИ принятие оперативных решений в ЦОДе – в том, конечно, случае, если ИИ будет надлежащим образом обучен работе на исторических данных. В 2024 г. положительный ответ на тот же вопрос дали уже только 58% из 557 опрошенных. Доверие к ИИ падает.

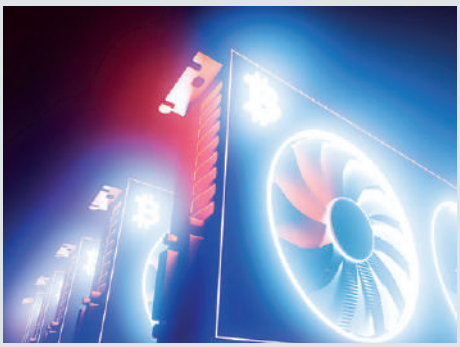
Перспективы ИИ важны для цодостроителей в первую очередь потому, что специфика работы соответствующих систем может обусловить повышение плотности мощности ИТ-стоек, а значит, изменение всей архитектуры дата-центров с внедрением прямого жидкостного охлаждения. Слово «может» здесь принципиально. Руководитель управления ЦОДов одного из крупных банков уверял меня, что ИИ-системы на базе GPU у них прекрасно работают в стойках мощностью до 20 кВт с воздушным охлаждением. А директор департамента НИОКР другого банка говорил о стоящей перед ним задаче по поддержке 350 (!!!) кВт на стойку. Столь широкий разброс показывает, что отрасль еще далека от выработки более или менее типовых требований относительно плотности энергопотребления. И что такое «ЦОД для ИИ», пока окутано туманом.

Понятно, ИИ – это уже наше настоящее. Но не стоит переоценивать его значение ни для экономики и жизни, ни для будущего ЦОДов.

За здоровый консерватизм,
Александр Барсков

ИТ-инфраструктура для ИИ → с. 38, 41

7 Вслед за инновациями



18 Легализация майнинга в России

ЦОД-2024. Время надежных

Рынок инженерных решений для ЦОДов адаптировался к санкциям и уходу западных вендоров. Основная борьба идет за восстановление доверия клиентов.

Организованный «ИКС-Медиа» 19-й ежегодный форум «ЦОД» вызвал небывалый ажиотаж – в нем приняло участие более 2 тыс. делегатов. Несмотря на перенос форума на более просторную площадку в бизнес-центр гостиницы «Рэдиссон Славянская», пространства для стендов и временных слотов для выступления всем желающим не хватило, и организаторам пришлось отказывать компаниям, не успевшим подать заявку в первых рядах. Доклады до вечера шли в шести потоках, и физически было невозможно посетить все интересные и подробно изучить представленные на выставке новинки. В кулуарах предлагалось перенести следующий форум в Лужники, в опросе Telegram-канала «ИКС-Медиа» 54% участников высказались за переход на двухдневный формат, а 3% – даже на трехдневный.

«До 2022 г. условия на рынке диктовали крупные игроки. Потом мы прожили непростые два года, когда ставка делалась на смелость – это было “время смелых”. Успеха добивались те, кто не струсил, остался и продолжал работать. Теперь мы переходим в стадию стабильности, которую называем временем надежных. Худшее, что принес 2022 г. – просадка доверия на рынке. Сейчас мы в стадии восстановления, и от наших с вами действий зависит, как процесс будет проходить дальше», – обратился к делегатам форума Максим Кыркунов, соучредитель компании C3 Solutions. Действительно, после ухода мировых лидеров с рынка инфраструктурных решений для ЦОДов, когда на первый план вышли азиатские компании, в том числе игроки второго эшелона, а также российские производители, пытавшиеся заполнить образовавшиеся ниши новыми для себя продуктами, доверие упало, и заказчики встали перед непростым выбором решений от поставщиков, не имевших долгой истории успеха.

Одним из инструментов выбора может стать «Карта вендоров решений для ЦОД», выпускаемая iKS-Consulting. Аналитическое агентство три года проводит опросы экспертов, технических директоров и проектировщиков крупных ЦОДов и по 30 параметрам оценивает потенциал и представленность вендора в инфраструктуре. По сути, карту можно считать отражением доверия крупных ЦОДов к вендорам инженерной инфраструктуры на российском рынке.

Российские стойки – проблем нет

Меньше всего проблем в импортозамещении стоек. В лидерах карты свежего выпуска – игроки, имевшие заметную долю на рынке и до 2022 г.: C3 Solutions, EMILINK и показавшая хороший рост ДКС. По-прежнему в ЦОДах представлены стойки Schneider Electric, хотя в будущее компании рынок уже не верит.

Зато участники рынка высоко оценивают потенциал возникшей на базе ее российской дочки компании Systeme Electric, возглавляющей рейтинг топ-10 (куда входят поставщики всего инженерного оборудования для ЦОДов). В наследство от мирового лидера российской компании остались экспертиза, квалифицированная команда и заводы в России. Так что есть возможности для роста, причем не только в сегменте стоек, но и в комплексных решениях. Директор коммерческого департамента управления по рынку «ИТ-решения» Systeme Electric Дмитрий Желтков сообщил, что «новая» российская компания реализовала в стране уже более сотни комплексных проектов.

Рынок ИБП – самый конкурентный

Больших успехов достигла Systeme Electric и на самом конкурентном рынке – ИБП. За год компания сделала рывок и по представленности вплотную подошла к лидеру, компании «Парус электро». Новичок первой тройки, компания Kehua Tech за прошедший год тоже добилась значительного прогресса. Среди ближайших преследователей – улучшившая за год позиции Huawei и совер-

шившая впечатляющий рывок компания ДКС, которая к изготавливаемым в Италии моноблокам добавила модульные решения китайского производства. Увеличив свою представленность, из левой части прошлогодней карты в середину переместились «Импульс», «Абитех Про» и C3 Solutions.

В середине карты – компании Ippon и Powercom, лидирующие на рынке ИБП по объему продаж. Это связано с методикой исследования – опрашивались технические директора крупных ЦОДов, а в этом сегменте компании представлены меньше. «На мой взгляд, на карте Ippon находится левее, чем должна быть. Причина по всей видимости в том, что клиенты из ЦОДов пока не в курсе того, что мы поставляем. Нам требуется сломать лед восприятия и доказать, на что способны», – прокомментировал результаты генеральный менеджер Ippon Михаил Вазисов. Потенциал у компании бесспорно высокий, особенно в сегменте мощных трехфазных ИБП, где игроков существенно меньше.

Заметно сдала позиции компания APC (Schneider Electric), которая до 2022 г. доминировала на нашем рынке. Клиенты не верят в потенциал и других ведущих мировых производителей, Vertiv и ABB, и переходят на российские и китайские решения. По характеристикам статические ИБП российской сборки не уступают продуктам мировых лидеров, но сохраняется зависимость от импортной силовой электроники и контроллеров. И по-прежнему на отечественном рынке не представлены динамические ИБП.

ДГУ: двигатели пока не из России

Другая проблемная позиция в импортозамещении систем энергоснабжения ЦОДов – ДГУ. Без помощи китайских заводов пока не обойтись, но и с ними надо уметь работать.

Лидер карты – компания ПСМ. «Мы реализуем свой подход к проектированию, производству и поставке дизель-генераторных установок, энергомодулей и комплектных трансформаторных подстанций для уже существующих проектов. Одно из передовых направлений компании – префаб-решения. В энергомодули можно устанавливать системы распределения питания, ИБП, АКБ и системы охлаждения. Это позволит масштабировать энергоцентр и запускать его очередями», – пояснил руководитель проектов ПСМ Антон Гущин.

Использование подготовленных на заводе модулей значительно сокращает сроки строительства. Например, ЦОД в Новосибирске на 440 стоек, по словам заместителя генерального директора компании «Свободные Технологии Инжиниринг» Юлии Колосковой, был построен за рекордные 11 месяцев. Такая скорость была достигнута в том числе за счет использования префаб-решений производства ART Engineering.

Второй в сегменте ДГУ идет компания «Хайтед», предлагающая также энергомодули высокой плотности. Замыкают первую тройку «ГрандМоторс» и Aksa Power Generation.

Никуда не делись уже установленные в ЦОДах ДГУ мировых лидеров: MTU (Rolls-Royce Solutions), Cummins и Mitsubishi. Самая важное в ДГУ – двигатель, которому по истечении определенного срока требуется капитальный ремонт. Бывший технический директор российского представительства Rolls-Royce Solutions, ныне генеральный директор «АБ Сервис» Константин Головишин предложил вместо капитального ремонта ДГУ в ЦОДе заменять только деградирующие со временем резинотехнические изделия, что существенно снижает стоимость жизненного цикла установки.

Электричество надо не только поставлять, но и распределять. Современным трендом в сегменте распределительных устройств, особенно важным для ЦОДов, стало уменьшение стоимости и габаритов решения по сравнению с традиционным. В частности, в таком ключе разрабатывает свои системы компания «АйТек», представившая цифровое комплектное распределительное устройство.

За связь без ошибок

СКС – один из самых динамичных сегментов рынка. За прошедший год компания EMILINK улучшила свою представленность и потенциал и занимает ведущую позицию на рынке. Резко прибавила компания Eurolan, размещающая заказы для ЦОДов на заводах в Израиле. Сохраняет свои позиции в тройке лидеров ДКС. Одним из секретов успеха компании руководитель отдела телекоммуникационных проектов ДКС Денис Горяченков считает финансовую стабильность. Несмотря на скачки курса доллара и 35%-ный рост цен на металл в 2023 г. компания до осени 2023-го не поднимала цены на оптические СКС, а до января 2024 г. – на корпусные решения.

Открытием года стали переместившаяся в правый верхний сегмент карты компания «Альфатек» и в середину – «ДАТАЛАН». За два последних года компании проделали большую работу и показали заметный рост. А вот в потенциал ранее считавшейся одним из лидеров этого сегмента рынка Panduit крупные заказчики уже не верят, да и представленность американской компании сильно уменьшилась.

Положительный момент – решения высокой и сверхвысокой плотности стали производиться в России. Насколько они соответствуют ожиданиям рынка, покажет время. Проблемой остается зависимость от импорта соединительных элементов и волоконно-оптических кабелей.

Холод из Китая

Растет нагрузка на стойки, растет мощность ЦОДов, повышаются требования к системам охлаждения. «Инфраструктура охлаждения должна обеспечивать высокую и регулируемую производительность, энергоэффективность и отказоустойчивость», – сформулировал генеральный директор компании TermoIndustry Денис Белоусов. Эксперт призвал обратить внимание на чиллеры Dunham-Bush, обеспечивающие, по его мнению, наилучшие показатели эффективности.

Впрочем, пока на весьма конкурентном российском рынке систем охлаждения для ЦОДов в центре внимания другие игроки. Стремительный рывок компании Envicool эксперты сравнили со взлетом ракеты. В этом году компания еще больше увеличила отрыв от конкурентов и уверенно занимает первое место. За год нарастила представленность на рынке компания «Рефкул», стремительно ворвалась в лидеры показавшая самый большой рост китайская TICA. Открытием года стала компания «Технофрост». Как ни удивительно, смогла нарастить и представленность, и оценку потенциала официально не присутствующая на российском рынке компания Stulz.

Системы охлаждения сильно зависят от качества комплектующих: компрессоров, вентиляторов, а изделия мировых брендов ограниченно доступны российским компаниям. Но на рынке есть и продукция, производимая на европейских заводах: в Россию легально поставляет кондиционеры и чиллеры вошедшая в китайскую Midea Group итальянская компания Clivet. «Важно, что мы на этой карте появились. Для нас это очень позитивный момент», – отметила председатель совета директоров Clivet Russia Вероника Сильвестрова. На российском рынке дата-центров о Clivet узнали недавно – головной офис компании дал разрешение на поставки в Россию систем охлаждения для ЦОДов только в конце 2022 г.

Российский рынок инфраструктуры для ЦОДов продолжает динамично меняться, и безоговорочных победителей нет. Растет доверие к российским и китайским компаниям, снижается – к мировым лидерам, без которых до 2022 г. рынок было трудно себе представить.

Новые и старые проблемы

Проблема выбора надежного вендора в условиях санкций и ухода с рынка мировых производителей – далеко не единственная, стоящая перед цодостроителями. В числе болевых точек, выделенных директором «РТК-ЦОД» по взаимодействию с органами государственной власти и организациями Дмитрием Паньшевым, – долгие сроки согласования и подключения энергетической мощности, выделения и оформления земельных участков и объектов недвижимости. Специфическая проблема – возможность попадания ЦОДа в зону комплексного развития территорий.

На проблемы многочисленных согласований накладываются финансовые – высокая ставка рефинансирования, увеличившаяся капиталоемкость ЦОДов. Срок окупаемости дата-центров вырос с трех-пяти лет до 10–15, что отпугивает инвесторов. «Высокая цена денег существенно сдерживает запуск новых крупных проектов и рост рынка. Ждем принятия мер поддержки отрасли», – заявил исполнительный директор «Ди Си Квадрат» Александр Мартынюк.

Есть проблемы с нормативной правовой базой. Так и не принят законопроект № 1195296-7 «О внесении изменений в Федеральный закон “О связи”», содержащий определение ЦОДа, нет разграничения ЦОДов с майнинговыми фермами, не введено понятие «облачные услуги».

Помимо этого, значительно выросли риски атак беспилотниками, о защите от которых стали задумываться даже на Дальнем Востоке. Также возможны атаки на объекты энергетики, поэтому даже самые рьяные противники использования ДГУ признали их необходимость в новых геополитических условиях.

В целом стоит отметить, что рынок инфраструктурных решений для ЦОДов адаптировался к санкциям. В кулуарах представители подсанкционных компаний говорили, что санкции практически не отражаются на финансовых результатах, более того, воспринимаются как своего рода знак «Герой труда», свидетельство того, что компания вносит весомый вклад в экономику страны.

Турбулентность на рынке сохраняется, появляются новые игроки, но уже начались процессы консолидации. В итоге, по мнению генерального директора сети дата-центров 3data Ильи Халы, в каждом из направлений останутся по три-четыре основных вендора, что будет свидетельствовать о зрелости рынка. Сейчас за то, чтобы попасть в эти списки, идет ожесточенная конкурентная борьба, причем прежде всего за счет повышения доверия клиентов. Наступило время надежных.

Николай Носов

Вслед за инновациями

7–10 октября в Алматы прошла неделя Data Center & Cloud Kazakhstan – уникальный комплекс мероприятий, включающий практические семинары, конференцию, выставку и двухдневный тренинг по тематике построения ЦОДов.

Ключевым событием «недели ЦОДов», посвященной вопросам цодостроения и предоставления облачных сервисов, стала конференция Data Center & Cloud Kazakhstan, которую «ИКС-Медиа» в этом году провела уже седьмой раз и которую посетили более 320 делегатов.

Совершенствованию цифровой инфраструктуры в Казахстане уделяется особое внимание на самом высоком уровне. Так, президент республики Касым-Жомарт Токаев в своем ежегодном послании подчеркнул необходимость активного развития телекоммуникационных сетей и дата-центров.

Жаксылык Ибрагимов

Для отрасли ЦОДов одним из ключевых изменений нынешнего года, как сообщил на конференции Жаксылык Ибрагимов, заместитель председателя Комитета телекоммуникаций Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан (МЦРИАП), стало внесение изменений в закон об информатизации, а именно определение понятий «центры обработки данных» и «облачные вычисления». Ранее оба термина отсутствовали в законодательстве, что затрудняло правовое регулирование этих сфер. «Центр обработки данных теперь официально закреплен в законодательстве как объект, обеспечивающий отказоустойчивое функционирование вычислительных ресурсов, телекоммуникационного оборудования и систем обработки данных. Законодательным закреплением мы закладываем фундамент для стабильного и структурированного развития рынка обработки и хранения данных», – отметил Ж. Ибрагимов.

Следующее важное для отрасли новшество – разработка правил по определению порядка организации деятельности ЦОДов и проведению международного и национального технического аудита. «Это добровольная оценка, которая будет проводиться для подтверждения уровня надежности инфраструктуры ЦОДов. Это шаг в направлении повышения доверия к инфраструктуре со стороны как государственных, так и частных заказчиков и инвесторов, которое, в свою очередь, будет способствовать развитию отрасли и привлечению на рынок новых участников», – пояснил представитель МЦРИАП.

Об уровне развития и зрелости отрасли ЦОДов в целом свидетельствуют показатели рынка коммерческих дата-центров. Согласно оценке iKS-Consulting, приведенной Светланой Черненко, генеральным директором Ассоциации операторов ЦОД и облачных сервисов РК, в 2023 г. в коммерческих ЦОДах Казахстана было размещено примерно 3,5 тыс. стоек. В текущем году это число увеличится незначительно, однако к 2030 г. эксперт ожидает существенного роста – возможно, до 10 тыс. стоек и более (рис. 1).

Росту количества стоек будет способствовать, в частности, реализация в Казахстане проекта ГК Key Point, который на конференции анонсировал основатель компании Евгений Вирцер. ЦОД, который планируется построить в Алматы и ввести в эксплуатацию во II квартале 2026 г., имеет проектную мощность 11 МВт (ИТ-мощность 6,2 МВт) и будет вмещать 880 стоек. Емкость первой очереди составит 440 стоек. Как и другие объекты сети Key Point, ЦОД в Алматы будет сертифицирован на соответствие требованиям надежности Tier III.

В числе предпосылок развития отрасли ЦОДов в Казахстане, помимо очевидного увеличения объемов хранения и обработки данных и усиливающегося в ИТ-отрасли тренда перехода от CAPEX-модели к OPEX, Е. Вирцер назвал выгодное географическое местоположение республики, которая может стать транзитным хабом между Китаем и Европой. Также все больше ЦОДов потребует обслуживание внутреннего спроса на контент и сервисы международных поставщиков, подразумевающее размещение их ресурсов на локальных казахстанских площадках.

Еще больше стоек добавит на рынок ЦОД Akashi, который должен быть построен в Астане. По плану его общая емкость – 4224 стойки, а сам ЦОД предполагается сертифицировать на соответствие Tier IV. Пока ЦОДа такого уровня нет не только в Казахстане, но и во всей Центральной Азии. Как сообщил Александр Захаров, технический директор Akashi Data Center, уже получена разрешительная документация и начато строительство. Первую очередь ЦОДа намечено ввести в эксплуатацию в конце 2025 г.

Облачный рынок как показатель инновационности

Что касается инфраструктурных облачных сервисов, то, по предварительным данным iKS-Consulting, в 2024 г. объем соответствующего рынка вырастет на 64,5%, до уровня 54,6 млрд тенге (рис. 2). Это существенно больше объема рынка услуг коммерческих ЦОДов, главным образом colocation, который составит 31,6 млрд тенге. Два-три года назад ситуация была обратной: доходы от colocation превышали доходы от облачных сервисов.

Ключевые факторы роста облачного рынка – увеличение числа новых пользователей и приток новых игроков. При этом государственные и квазигосударственные компании формируют больше половины спроса.


Светлана Черненко

Вовлеченность бизнеса в цифровизацию, аутсорсинг ИТ и инновации в принципе остается весьма слабой. По оценке С. Черненко, проникновение облачных сервисов в корпоративном секторе находится на уровне 10%. Это соответствует общему уровню внедрения инноваций на предприятиях, что серьезно тормозит развитие рынка облачных сервисов и коммерческих ЦОДов в целом.

Ситуация может измениться благодаря реализации принятого летом 2024 г. Национального плана развития Республики Казахстан до 2029 г. Согласно плану, инновационность экономики – основной фактор социально-экономического развития страны, и почти в каждом пункте упоминается смещение акцентов с сырьевой направленности на инновационную. В числе приоритетов, указанных в документе, – развитие цифровой инфраструктуры, что может существенно повысить спрос на объекты хранения и обработки данных.

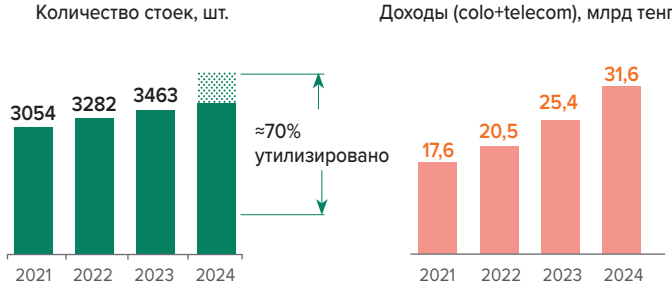
Плюсы и минусы дата-хаба

Еще одна важная инициатива руководства страны – создание в Казахстане среднеазиатского дата-хаба, названное президентом К.-Ж. Токаевым одной из приоритетных целей цифрового развития республики. По замыслу, дата-хаб должен стать центром притяжения мировых поставщиков облачных технологических решений, приблизив их к потенциальным пользователям как из Казахстана, так и из соседних государств.

Понятно, что для привлечения big-tech-компаний в регион требуется построить соответствующую физическую инфраструктуру хранения данных для размещения оборудования и развертывания локальных облачных платформ гиперскейлеров. Это, в свою очередь, потребует создания новых площадок и обеспечения их необходимыми энергетическими мощностями.

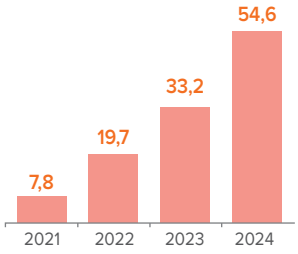
Однако, как отмечают эксперты, подходы, которые могут быть использованы для решения поставленных за-

Рис. 1. Текущее состояние рынка коммерческих ЦОДов в Казахстане ▼



Источник: iKS-Consulting

Рис. 2. Объем рынка облачных инфраструктурных сервисов Казахстана, млрд тенге ▼



Источник: iKS-Consulting

дач, могут оказать как положительное, так и отрицательное влияние на локальный рынок, в связи с чем требуется тщательная проработка всех возможных сценариев формирования дата-хаба.

Среди очевидных плюсов – укрепление имиджа Казахстана на мировом ИТ-рынке, реализация транзитного потенциала страны, создание рабочих мест для казахстанских ИТ-специалистов. Кроме того, такой проект будет способствовать росту популярности сервисной модели использования ИТ, стимулирует конкуренцию на рынке облачных услуг и строительство новых ЦОДов, повысит спрос на услуги colocation.

Но возможны и негативные эффекты. Это, в частности, каннибализация местного облачного рынка, отток капитала и недополучение налоговых отчислений бюджетом Казахстана. Построение гиперЦОДов может в долгосрочной перспективе вызвать дефицит электроэнергии в стране и ухудшить экологическую ситуацию. «Казахстан может стать ресурсной базой, а не бенефициаром выгод от создания дата-хаба», – предупредила С. Черненко.

Мода на ИИ

Среди технологических аспектов, связанных с построением ЦОДов, на конференции наиболее активно обсуждалась подготовка к массовому внедрению систем искусственного интеллекта. По оценке компании Schneider Electric, которую привел Денис Вайнер, ее директор по продажам в Центральной Азии, Азербайджане и Грузии, если в 2023 г. на системы ИИ приходилось около 8% установленных в ЦОДах ИТ-мощностей, то к 2028 г. это показатель вырастет до 15–20%. Причем, если сегодня до 95% рабочей нагрузки ИИ-систем ложится на головные ЦОДы, то к тому же 2028 г. она будет поровну распределена между головными и периферийными (edge-) ЦОДами.

Специфика обучения ИИ-моделей и высокие требования к производительности заставляют повышать энергетическую мощность стоек до десятков и даже сотни киловатт. «Мы находимся в точке перехода. Тепловая мощность процессоров растет и будет расти. Традиционные системы охлаждения необходимый теплоотвод обеспечить не могут. Их предел – при правильном проектировании – 30–40 кВт. 50 кВт – тупик для любого воздушного охлаждения. Далее либо жидкостное охлаждение, либо переход на процессоры, которые могут работать при более высоких температурах», – дал свой прогноз Д. Вайнер.

На специальном семинаре, проведенном в рамках недели Data Center & Cloud Kazakhstan, компания Schneider Electric представила разработанное совместно с Nvidia эталонное решение для высокоплотных инсталляций. Оно предусматривает четыре варианта: три для уже существующих объектов и один для вновь строящихся. Гибридный подход, сочетающий воздушное и прямое жидкостное охлаждение, обеспечивает подачу электропитания и отвод до 73 кВт тепла с одной стойки. Обещано в начале 2025 г. расширить этот диапазон до 123 кВт.

Переход на высоконагруженные стойки отражается почти на всех системах ЦОДов. Цодостроители все активнее экспериментируют с альтернативными источниками электроэнергии, пробуют разные подходы к времени автономной работы. Большой интерес аудитории вызвало представленное компанией Piller решение на основе водородных топливных элементов, вошедшее в ее портфель в результате покупки итальянской фирмы GKN Hydrogen. По словам Владислава Ротаня, менеджера по продажам Piller, такие решения применяют все чаще, особенно для удаленных объектов.

Достоинства решения Piller – эксплуатация в естественных температурных условиях и низкое давление в ячейках (0,5–40 бар). А к числу преимуществ водородных топливных элементов в целом следует отнести длительный срок службы (30 лет и более), отсутствие саморазряда и почти неограниченное количество циклов заряда – разряда. Главный недостаток – высокая стоимость, и пока он перевешивает все преимущества.

Однако сам интерес аудитории к подобным решениям показывает готовность отрасли ЦОДов к инновациям. У казахстанских коллег есть важное преимущество – им доступны все мировые разработки, чего россияне, увы, лишены из-за санкций. Это преимущество наряду с государственной поддержкой и ростом интереса инвесторов формирует основу для ускоренного развития отрасли ЦОДов в Казахстане.

Александр Барсков
Алматы – Москва

НОВОСТИ АНО КС ЦОД

АНО КС ЦОД получила образовательную лицензию

11 июня АНО «Координационный совет по ЦОДам и облачным технологиям» получила лицензию на осуществление образовательной деятельности. Это результат более чем трехлетней работы по созданию обучающих программ, которые уже заслужили высокие оценки отраслевых специалистов. Сейчас действуют шесть образовательных программ, в которых рассматриваются различные аспекты проектирования, строительства, эксплуатации ЦОДов и отдельные их подсистемы: электрические, механические, телекоммуникации и сети. «Получение образовательной лицензии позволит охватить больший круг специалистов, заинтересованных в получении практических знаний в области инфраструктуры дата-центров и услуг на их базе. Мы и дальше будем расширять перечень программ обучения. В этом году появился новый курс по сетям и телекоммуникациям в ЦОДе, в следующем году планируем провести первое обучение по облачным технологиям», – сообщил генеральный директор АНО КС ЦОД Дмитрий Бедердинов.

Отечественная модель классификации эксплуатации ЦОДа

15 августа прошло совещание рабочей группы АНО КС ЦОД по обсуждению документа «Модель классификации эксплуатации ЦОДа». В формате открытого диалога были обсуждены ключевые вопросы и предложения коллег. Большая часть представленных ранее рекомендаций учтена и будет включена в окончательную редакцию текста.

Разрабатываемая модель поможет оценить уровень компетенций специалистов службы эксплуатации, внедрить рейтинговое и представленное публично ранжирование дата-центров по классам эксплуатации. Она должна помочь потребителям услуг ЦОДов сделать обоснованный выбор, а владельцам и операторам ЦОДов – оценивать уровень квалификации сотрудников и зрелость процедур эксплуатации, а также совершенствовать их для повышения качества предлагаемых услуг.

Тренинг в Алматы

9–10 октября АНО КС ЦОД провела в Алматы обучающий курс «Построение ЦОДов». Этот тренинг проводился второй раз и, как и первый год назад, – в рамках «недели ЦОДов», серии связанных между собой посвященных ЦОДам и облачным сервисам мероприятий, включая форум Data Center & Cloud Kazakhstan.

Рынок услуг ЦОДов и облачных сервисов в Казахстане входит в новую фазу развития: растет количество проектов, новых площадок ЦОДов, появляются новые игроки. На ежегодных конференциях «ИКС-Медиа» в Алматы регулярно говорят о дефиците профессиональных кадров, и многие специалисты обращались с пожеланиями регулярно проводить в республике тренинги, которые уже несколько лет с большим успехом проходят в России.

Классификация ЦОДов: от модели к ГОСТу

23 октября состоялась встреча членов АНО КС ЦОД, на которой обсуждалась необходимость разработки нового ГОСТа по классификации инженерной инфраструктуры ЦОДов. По итогам принято решение начать разработку государственного стандарта, создать рабочую группу и привлечь профессиональных экспертов и организации для прохождения процедур согласования.

НОВОСТИ ОТРАСЛИ

Инвестиции в подмосковные ЦОДы

Объем инвестиций в выполняемые на территории Московской области крупные проекты создания ЦОДов составляет 95 млрд руб. Осуществить заявленные крупные проекты планируется до конца 2027 г. Об этом на площадке XI Международного форума технологического развития «Технопром-2024» рассказала заместитель председателя правительства – министр инвестиций, промышленности и науки Московской области Екатерина Зиновьева. Она отметила, что сегодня Московская область занимает третье место среди российских регионов по количеству действующих ЦОДов. На территории региона сейчас функционируют 12 центров обработки данных.

«РТК-ЦОД» построит дата-центр в Хабаровском крае

«РТК-ЦОД» подписала соглашение с Корпорацией развития Дальнего Востока и Арктики о строительстве нового центра обработки данных на площадке территории опережающего развития «Ракитное» в Хабаровске. Проект дата-центра включает в себя четыре машзала общей емкостью 440 стойко-мест и подведенной мощностью 4 МВт. Проектирование объекта начнется в 2025-м, а ввод в эксплуатацию запланирован на III квартал 2027 г. Объем инвестиций в проект составит 1,4 млрд руб.

Российский рынок облачной инфраструктуры к 2028 г. может превысить 460 млрд руб.

Согласно аналитическому отчету iKS-Consulting «Текущий статус и потенциал развития российского рынка облачных инфраструктурных сервисов и колокации до 2028 г.», в ближайшие пять лет рынок облачных инфраструктурных сервисов в России увеличится в 3,8 раза, рынок колокации – в 2,4 раза. По оценкам аналитиков, объем российского рынка облачных инфраструктурных сервисов в 2028 г. достигнет 464 млрд руб. (в 2023 г. – 121 млрд руб.). Это соответствует среднегодовому темпу роста 30,7%. Рынок инфраструктурных облачных сервисов делится на два основных сегмента, лидирующие позиции с долей 77% к 2028 г. сохранит IaaS.

Россия пока заметно отстает от других стран БРИКС и Большой семерки по уровню проникновения облачных сервисов в соотношении с ВВП, что говорит о большом потенциале роста, который может быть успешно реализован на фоне продолжающейся цифровой трансформации в стране. К 2027 г. этот показатель увеличится более чем вдвое.

ГК Softline и ГК Key Point договорились о создании сети модульных ЦОДов

На IX Восточном экономическом форуме подписано трехстороннее соглашение о сотрудничестве между Корпорацией развития Дальнего Востока и Арктики (КРДВ), ГК Key Point и ГК Softline. Соглашение предусматривает создание сети масштабируемых модульных ЦОДов, полностью оснащенных ИТ-инфраструктурой, в регионах ДФО и Сибири. Объединение компетенций и возможностей Key Point и Softline при поддержке КРДВ поможет увеличить объемы оказываемых ИТ-услуг в регионах. Создание модульных ЦОДов и развертывание ИТ-инфраструктуры планируется в республиках Якутия и Бурятия, Хабаровском, Забайкальском и Камчатском краях, Сахалинской, Амурской и Магаданской областях, в Чукотском автономном округе.

Nubes запустил второй ЦОД

Источник: Nubes

Облачный провайдер Nubes открыл ЦОД Strato на юге Москвы. На базе дата-центра компания будет предоставлять облачные сервисы и услуги размещения клиентского оборудования. ЦОД Strato расположен рядом с первым объектом Nubes – ЦОДом Alto, открытым в 2022 г., однако дата-центры компании независимы друг от друга на уровне всех систем.

Новый ЦОД рассчитан на размещение 198 стоек мощностью до 15 кВт – таких показателей позволяют добиться изоляция холодных коридоров, использование специальной плитки и ряд других мер. По словам генерального директора Nubes Василия Степаненко, ЦОД Strato, как и уже действующий Alto, соответствует уровню Tier III.

СВОБОДНЫЕ
ТЕХНОЛОГИИ
ИНЖИНИРИНГ

ПРОСТЫЕ РЕШЕНИЯ СЛОЖНЫХ ЗАДАЧ

ПРОЕКТИРОВАНИЕ И СТРОИТЕЛЬСТВО ДАТА-ЦЕНТРОВ

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

+7 (495) 120-28-66

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

«Всё в наших руках!»

Евгений Вирцер

ЦОД Key Point во Владивостоке – первый ЦОД Tier III на Дальнем Востоке

В преддверии пятилетия компании «Свободные Технологии Инжиниринг» (СТИ) «ИКС» беседует с ее основателем и генеральным директором Евгением Вирцером.

– Евгений, с чего все начиналось?

– Компания была зарегистрирована 29 ноября 2019 г., а первый рабочий день случился 10 января 2020 г. На работу в тот день вышел один сотрудник – я (*улыбается*). Первоначально в нашей команде было семь-восемь человек. В основном это были люди, с которыми мы много лет до этого проработали вместе, прошли, как говорится, огонь, воду и медные трубы, хорошо знали не только профессиональные, но и человеческие качества друг друга (что даже важнее). Сегодня компания сильно разрослась, в штате уже 320 человек, многие из которых росли как специалисты вместе с СТИ и сегодня занимают руководящие должности.

– Что значит слово «свободные» в названии компании?

– Честно говоря, когда мы придумывали название, не вкладывали в него какого-то глубокого смысла. Сейчас, конечно, можно сказать, что мы «свободны» от технологических предрассудков, что у нас нет слепой привязанности к каким-либо технологиям, что все зависит от задач, которые ставятся в конкретном проекте.

– Можете кратко сформулировать, чем занимается компания?

– Если официально, то проектированием и строительством ЦОДов. Изначально понимали, что ЦОДы будут нашим основным «центром тяжести». Так и получилось. Хотя занимаемся и другими проектами – комплексными инженерными системами, скажем так, на нетривиальных гражданских объектах.

– Когда вы создавали компанию, наверняка был бизнес-план. Насколько он выполнен, перевыполнен?

– Создание СТИ стало результатом определенных обстоятельств, и не могу сказать, что у нас сразу был четкий бизнес-план с конкретными финансовыми показателями. С самого начала мы, небольшая группа компетентных людей, известных на рынке, понимали, что новой компании будет сложно получать какие-то крупные проекты, что будем пробиваться постепенно. Да и о каком плане могла идти речь, когда через пару месяцев после начала работы компании объявили карантин из-за пандемии? Потом СВО, жесточайшие санкции, скачки валютных курсов… Так что почти все время своего существования компания работает в очень сложных условиях. Это нас закалило и, возможно, помогло нам стать теми, кем стали.

Помню, в августе 2020 г. мы кругом из нескольких человек собрались в неформальной обстановке, чтобы обсудить, чего в профессиональном плане в новой компании хочет каждый из нас, какова цель компании. Кто-то сформулировал: «Хотим через четыре года стать лучшими цодостроителями в стране». Улыбнулись, забыли. Четыре года прошло, вспомнили и подумали, что, похоже, получилось стать если не лучшими, то одними из лучших. Хотя четкого плана достижения этой цели не было. Работали по принципу: в любой ситуации надо делать максимум возможного.

Если говорить про экономические показатели, то последние несколько лет фиксируем в среднем трехкратный ежегодный рост. В этом году, полагаю, уже так сильно не вырастем, рост будет более плавный. Опять же четких финансовых планов, что в 2025-м должны вырасти на столько, в 2026-м – на столько, у нас нет. Есть серьезный портфель контрактов на 2025–2026 гг., и точно появятся еще проекты, которые мы пока не учитываем. Главный план – реализовать все проекты так, чтобы ими можно было гордиться. Стремясь создать идеальный ЦОД.

– Что такое идеальный ЦОД?

– Для меня идеальный ЦОД – тот, который не строится, а собирается, как некий конструктор. Но мы еще только в начале пути к такому ЦОДу. Когда дойдем, это будет мини-революция в цодостроении у нас в стране. Понятно, что идеальный ЦОД должен работать без внеплановых остановок. Надежность – ключевая характеристика таких объектов. И, безусловно, ЦОД должен доставлять эстетическое удовольствие тому, кто там находится. Промышленный дизайн – очень крутая штука.

– А финансовая сторона?

– Финансы – это даже не обсуждается, это основа любого проекта. Проект должен быть конкурентен по цене, по срокам. Мы не строим воздушные замки, которые стоят в 10 раз дороже, чем принято на рынке. Проект должен и заказчика устраивать с точки зрения цены, и нам давать заработать.

– Каковы главные ценности для СТИ как компании?

– Первое – не идти на компромисс в технологических принципах, в профессионализме, не обманывать, быть честными. Для нас во главе угла – принципы, если хотите, справедливая формула, а потом – цифры, которые следуют из этой формулы. Какие бы они ни были, если формула справедливая, значит, цифрам надо доверять. Часто приходится сталкиваться с тем, что люди, наоборот, пытаются формулу «натянуть» на цифры – это неправильно.

Второе – у всех наших партнеров, равно как и у сотрудников, всегда есть право на ошибку. Ошибаются все. Ошибся – исправься, и пошли дальше. Точку в отношениях из-за ошибок мы не ставим. Это еще один принципиальный момент работы нашей компании. К тому же я четко осознаю, что самые тяжелые ошибки всегда мои собственные.

Отсюда переходим к самой главной нашей ценности – к команде. Нам удалось собрать под одной крышей уникальный коллектив, который может решать самые сложные задачи и, что очень важно, получать от этого удовольствие и продолжать ставить себе новые цели. Это сильные личности и абсолютные бойцы по характеру, которыми я искренне восхищаюсь.

– Назовите проекты, которыми вы гордитесь. И проекты, о которых хочется забыть.

– Проекты, о которых хочется забыть, есть у всех – это нормально, но о них мы забыли, хотя выводы для самих себя сделали.

Гордимся каждым построенным нами ЦОДом. Сегодня введены в эксплуатацию четыре таких объекта: это ЦОДы Key Point во Владивостоке, в Новосибирске и два в столице: N1 и «Москва-2». Дата-центр «Москва-2» стал первым в России объектом, получившим сертификат Tier IV – конечно, гордимся. У каждого из этих проектов своя интересная судьба, и с каждым связан свой набор сложностей, которые нам приходилось преодолевать.

Если говорить не про ЦОДы, то гордимся новым кампусом МГТУ им. Баумана, который в сентябре 2024 г. был открыт с участием президента России и мэра столицы. Очень большой, сложный объект. Мы проектировали там все инженерные системы, часть систем строили. Когда туда прихожу, прямо мурашки по телу, для меня Бауманка сопоставима с космодромом, который делали еще «в прошлой жизни». Это объекты одного уровня в плане значимости для страны и наследия для людей.

ЦОД «Москва-2» – первый ЦОД Tier IV в России

– За какие проекты принципиально не беретесь?

– Когда заказчик неоправданно, с нашей точки зрения, считает себя более компетентным, чем мы. Бывают ситуации, когда заказчик действительно намного хуже нас разбирается «в теме», но при этом пытается излишне участвовать во всех этапах проекта. Это очень тормозит весь процесс, и так работать нельзя. Мы стараемся получить от заказчика техническое задание с основными параметрами ЦОДа. Есть ТЗ, есть бюджет, есть сроки – дальше наша задача.

При этом мы, конечно, прислушиваемся к заказчику, ничего от него не скрываем, показываем всю подноготную проекта, но принятие технических и управленческих решений всегда остается за нами. Если заказчик нам не доверяет и с ним надо согласовывать каждый чих, в такие истории мы не ввязываемся. Это просто потеря времени. Не значит, что такие проекты нельзя довести до конечного результата. Можно, но времени придется потратить в два раза больше. А временем своим мы дорожим. Интересных проектов много.

ЦОД Key Point в Новосибирске – крупнейший коммерческий ЦОД за Уралом

Кроме того, делаем только проекты под ключ: не идем отдельно в проектирование, отдельно в построение какой-либо системы или группы систем.

– Кто ваши основные конкуренты? Они вообще есть?

– Если говорить о формальной стороне конкуренции, то она, конечно, есть. Ведь есть компании со схожими компетенциями, которые работают на том же рынке. Мы вместе с ними участвуем в конкурсах.

Но сегодня работы на рынке намного больше, чем компетенций. Проектов много, и часто лучше не конкурировать, а объединять компетенции. Приведу в качестве примера наши отношения с компанией «АМДтехнологии», к компетенциям которой относимся с большим уважением. В каких-то проектах мы конкурируем. Но сейчас два больших проекта делаем совместно. Для меня это важная история, потому что инициатива изначально была моя. На этих объектах мы являемся генподрядчиком, а они занимаются охлаждением. Так случилось не потому, что мы не умеем делать данный вид работ, а потому, что решили попробовать такой формат взаимодействия. Искренне хочу, чтобы все реализовалось так, как задумали, и дальше будем продолжать сотрудничать.

В целом ярко выраженных конкурентов у нас сегодня нет. И не потому, что мы «великие», а потому, что задач на рынке больше, чем реальных возможностей. Самый большой наш конкурент – мы сами. Только мы сами можем себе навредить и сделать хуже. Но в наших силах этого не допускать.

– На что переключитесь, когда построите все ЦОДы или когда строить их будет невыгодно?

– Как я уже говорил, наша компетенция – инженерные системы и управление проектами. Если ЦОДы все закончатся, будем заниматься другими интересными объектами – промышленными, транспортными... Опыт у команды есть, переключимся. Но, думаю, на наш век ЦОДов хватит (*улыбается*).

– Сколько ЦОДов сейчас у вас в работе, в стадии проектирования или строительства?

– В несколько раз больше того, что уже построено. Суммарная емкость введенных нашей компанией в эксплуатацию ЦОДов – около 5,5 тыс. стоек, 55 МВт установленной мощности. А в проектировании и строительстве сейчас проекты общей емкостью более 14,5 тыс. стоек, или примерно 213 МВт мощности.

– Для отрасли цодостроения характерна кадровая проблема. Как ее решаете? По какому принципу формируете команду?

– С кадрами всегда было сложно, для нас особенно в начале нашей работы. Привлекать хороших специалистов было непросто, компания была маленькая, не на слуху, а в пандемию люди не хотели уходить с насиженных мест.

Сейчас проще. Уровень компании совсем другой, в портфеле у нас много крупных и интересных проектов. Возвращаясь к ценностям компании: не буду говорить, что мы – одна семья, но лояльность сотрудников к тому, что делает компания, и лояльность компании к сотрудникам очень важны. У нас любой руководитель доступен для любого сотрудника, двери всегда открыты. И еще важно не

только привести в коллектив профессионала, важно, чтобы он встроился в нашу идеологию, разделял наши ценности. Важна внутренняя атмосфера, чтобы у сотрудников была комфортная среда для работы. Но не всегда профессионалы высокого уровня могут вписаться в сложившийся коллектив.

Конечно, стремимся воспитывать кадры внутри компании, поскольку свой сотрудник всегда лучше, чем даже более профессиональный в моменте, но пришлый «варяг». Надо помогать своим сотрудникам двигаться по карьерной лестнице, развивать их компетенции, помогать им расти.

Еще один важный момент: мы открыли в МЭИ базовую кафедру «ЦОД» на базе Института энергоэффективности и водородных технологий. С этим вузом уже более двух лет сотрудничаем в сфере BIM-проектирования, читаем лекции, открыли аудиторию по BIM-технологиям – лабораторию цифрового проектирования. А теперь еще будет кафедра. В феврале начнутся занятия. Там будет несколько дисциплин: электрические системы, механические системы, слаботочные системы, эксплуатация, управление строительством, сертификация и ввод объектов в эксплуатацию.

Этот проект для нас абсолютно не коммерческий, мы тратим на него собственные средства и делаем это осознанно. Бессмысленно ждать, что кто-то придет, взмахнет волшебной палочкой и насытит отрасль квалифицированными кадрами. Мы считаем, что формирование кадров для отрасли – это в том числе и наша задача и миссия, и искренне надеемся, что подобных инициатив от участников рынка с каждым годом будет больше.

ЦОД «Москва-2» – первый ЦОД Tier IV в России

– Последние годы были непростыми для рынка. Что сегодня является главным тормозом вашего бизнеса и отрасли ЦОДов в целом?

– Если говорить непосредственно о сегодняшнем дне, то, конечно, ключевая ставка ЦБ и стоимость денег. Дешевые деньги – залог развития любой экономики, любой отрасли. Это первое.

Второе – непростые условия приобретения, доставки и сервисного обслуживания оборудования. Уровень сервиса не такой, к какому привыкли. Но вздыхать и охать все уже перестали, ситуация такая, какая есть.

И третье: для нас всегда большая проблема – нехватка компетентных подрядчиков. Но она решаема. Дорожим теми, кто хорошо себя проявляет, задействуем их в новых проектах.

ЦОД N1 (Москва, Tier III)

– Если санкции отменят и ушедшие западные производители вернутся, будет легче?

– Им надо будет очень постараться, чтобы закрепиться на рынке. Уже есть несколько ниш по оборудованию, где мы определились с партнерами. И нам с ними комфортно. Наше партнерство выходит за рамки отношений «производитель – покупатель», у нас общая философия, взгляды на ведение бизнеса. Ведь ответственные партнерские отношения могут компенсировать какие-то технические огрехи, если они возникают.

Есть ряд российских производителей, которые вкладываются в развитие, у которых свой мощный НИОКР, которые прислушиваются к нашему мнению. Это не конъюнктурщики, они видят себя на этом рынке вдолгую. Плюс у них очень достойные продукты. В качестве примера могу назвать наших технологических партнеров и крупных российских производителей – компанию «Парус электро», за-

Новый кампус МГТУ им. Баумана

вод ПСМ, компанию ДКС. Мы совместно выполнили уже не один проект и планируем продолжить сотрудничество. С такими производителями мы стараемся формировать экосистему единомышленников.

– Говоря про экосистему, следует сказать, что вокруг СТИ за эти годы появился ряд смежных проектов.

– Да, действительно, СТИ трансформировалась в группу технологических компаний, каждая из которых осваивает свою нишу на рынке ЦОДов. СТИ – центр компетенций по инженерным системам и управлению строительством. ART Engineering занимается производством оборудования для ЦОДов, Key Point – первая в стране сеть коммерческих операторонезависимых ЦОДов.

На «Карте вендоров ЦОД», составляемой iKS-Consulting, ART Engineering – один из самых быстрорастущих брендов. Да и в финансовом плане в относительных значениях компания растет быстрее, чем СТИ. Думаю, в 2025–2026 гг. этот опережающий рост продолжится.

Key Point как сеть ЦОДов мы мечтаем сделать российским «Эквиниксом» (транснациональная компания Equinix – один из мировых лидеров среди colocation-провайдеров. – *Прим. ред.*). Не обязательно по финансовым показателям или числу стоек. А в первую очередь по качеству объектов, их надежности, по использованию передовых технологий, по восприятию заказчиков.

– Каковы цели компании на следующую пятилетку?

– Цели пока не формализовали, но их будет несколько. Одна из них – выйти на международный рынок. И не только на рынок СНГ – о проекте в Казахстане мы уже объявили. В горизонте пяти лет хотим реализовать проект в дальнем зарубежье. Надеюсь, на зарубежных рынках помимо экспертизы СТИ будет востребована продукция ART Engineering. Добиться этого – серьезная задача. Но если сформируем конкурентный продукт, способы ее решения найдем.

Другая, не менее важная цель – сохранить и упрочить лидерство на российском рынке цодостроения. Забраться на гору было нелегко, но удержаться еще сложнее. Поэтому сегодня важно изыскивать внутренние резервы, наращивать экспертизу, продолжать поиск новых решений и улучшать существующие, самосовершенствоваться, чтобы завтра быть на несколько шагов впереди и предвосхищать потребности рынка.

Наша главная цель – делать лучшие ЦОДы. Трезво смотрю на вещи: любой наш объект можно сделать лучше. Даже когда получилось очень хорошо, всегда есть понимание, что можно было сделать еще лучше. Все в наших руках.

Легализация майнинга в России: первый шаг сделан

Бизнес в целом положительно оценил принятые Госдумой поправки в законы, регулирующие майнинг. Многое будет зависеть от дальнейших действий Банка России.

Николай Носов

Мировая финансовая система находится в кризисе. Необеспеченные триллионные вливания долларов в ведущую экономику мира приводят к экспорту инфляции в другие страны. Заморозка и возможная конфискация российских активов подрывают доверие к единой финансовой системе в странах третьего мира, осознавших, что легко могут стать следующими. Нет доверия к доллару, нет доверия к финансовым институтам, к договоренностям и выработанным правилам. Неудивительно, что становится востребованной обеспечивающая доверие в недоверенной среде технология блокчейна и растет популярность созданных на ее базе криптовалют.

Лед тронулся

Хайп вокруг технологии блокчейна прошел, ее перестали применять везде где можно только потому, что это модно. Но сама технология осталась, никуда не делись и криптовалюты. Курс биткоина относительно доллара, хотя и претерпевал существенные падения, вырос по сравнению с 2020 г. в четыре раза. Аналитики всерьез обсуждают использование биткоина в качестве резервной валюты в стране.

«Консенсус, основанный на золотом запасе, становится неустойчивым. Бессмысленно хранить в Форт-Ноксе золото, если его в любой момент могут конфисковать. В мире нет доверия к некогда классическим инструментам, и криптовалюты обсуждаются на самом высоком уровне. Биткоин – средство идентификации реального объекта в цифровом мире. Если биткоин станет аналогом золотовалютного запаса, то нужно технологически контролировать сеть, чтобы без вас не могли провести конфискацию – переложить “цифровое золото” из одного кармана в другой. Поэтому майнинг при нахождении оборудования на территории страны имеет стратегическое значение, в том числе с точки зрения формирования новой платежной системы для мирового сообщества», – дал комментарий нашему изданию интернет-омбудсмен Дмитрий Мариничев.

В 2023 г. Россия впервые вышла на второе место по мощностям для майнинга криптовалют, уступив только США. Но до настоящего времени бизнес находился в серой зоне, что приводило к созданию подпольных майнинговых ферм, использующих льготные тарифы для населения, проблемам с электричеством, уклонению от уплаты налогов. Даже легальные, платящие по промышленным расценкам за электроэнергию майнинговые фермы свою деятельность старались не афишировать.

Наше издание уже писало о необходимости введения майнинга в правовое поле и легализации криптовалют для внешнеэкономической деятельности. Никто не призывал использовать криптовалюту для внутренних расчетов – для этого есть рубль, а преимущества криптовалют реализует активно внедряемый цифровой рубль. Но для внешнеэкономической деятельности, особенно в условиях санкций, применение криптовалюты в расчетах выглядит перспективно. В долларах тоже нельзя проводить внутренние расчеты, а тот же биткоин, в отличие от американских фиатных денег, не эмитируется недружественной страной.

Первое обсуждение криптовалют состоялось в Госдуме еще в 2016 г. Но реальным регулированием занялись только сейчас, с принятием двух взаимосвязанных законов. 30 июля 2024 г. Госдума одобрила во втором чтении законопроект, позволяющий Банку России с 1 сентября запустить эксперименты по созданию в РФ площадки для использования криптовалют в международных расчетах. Также разрешаются биржевые торги криптовалютой и создание оператора по расчетам в них в контуре Национальной платежной системы. Следом был принят так называемый закон о майнинге (Федеральный закон от 08.08.2024 № 221-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»), закрепляющий порядок и условия осуществления майнинга в стране.

Майнинг и валютный контроль

Как Центробанк будет реализовывать предоставленную законодателями возможность, пока неизвестно. Но, исходя из предыдущего опыта и стремления Центробанка поставить под контроль пересекающие границу финансовые потоки, можно сделать предположения.

Прежде всего, ЦБ РФ придется вписать криптовалюты в процедуры валютного контроля, обеспечивающего выполнение валютного законодательства. Осуществляя контроль, регулятор проверяет поступления и списания денежных средств по валютным счетам. То есть при расчетах в криптовалютах у участников внешнеэкономической деятельности должны быть криптокошельки, или, в терминологии нового закона, «адреса-идентификаторы», зарегистрированные в Центробанке. Легальными будут признаваться только платежи через них, а регулятор должен иметь возможность видеть операции и остатки средств.

Это требование накладывает ограничения на используемые криптовалюты. Впрочем, для наиболее распространенных Bitcoin и Ethereum проблем здесь нет. Анонимность распространяется лишь на владельца кошелька, а не на его содержимое. Скорее всего, по аналогии с рублями Центробанк будет открывать предприятиям основной криптокошелек (валютный счет) и транзитный (транзитный счет), на который будут поступать средства. А для борьбы с отмыванием доходов и финансированием терроризма будет вестись список криптокошельков, подозреваемых в нарушениях. Однако с учетом специфики криптовалют и простоты создания криптокошельков делать это будет довольно сложно.

Криптовалюту как имущество предприятия смогут легально покупать за рубли у внесенных в реестр майнинговых компаний, а не у серых посредников в Москва-Сити. Остается отработать вопрос, как предприятия смогут продавать полученную за свои товары криптовалюту. Возможно, придется вернуться к вопросу легализации криптовалютных бирж.

Первый шаг

В целом связка законов положительно оценена рынком. «Нет предела совершенству, есть что подкручивать и изменять, но это хороший первый шаг», – отметил Д. Мариничев в эфире канала МК ТВ. Его мысль продолжил Олег Огиенко, заместитель генерального директора по коммуникациям компании BitRiver: «Мы воспринимаем принятый закон как закон о развитии отрасли. Его ждали много лет. Это официальный старт развития отрасли, институционализация инвестиций в данную сферу».

Важно, что в новом законе введены правила и определения. Заниматься майнингом смогут российские юрлица и индивидуальные предприниматели, включенные в реестр лиц, осуществляющих майнинг цифровой валюты, или в реестр операторов майнинговой инфраструктуры. Россиянам, не имеющим статуса ИП, разрешено заниматься майнингом без включения в реестр до тех пор, пока они не превышают установленные правительством лимиты энергопотребления.

Логичное решение – правительство сможет вводить запрет на майнинг в отдельных регионах или на их отдельных территориях и с учетом местных особенностей ограничивать, полностью или частично, энергопотребление майнерами. Майнеры не должны создавать проблем для населения и промышленных предприятий.

Нарушение запрета и ведение майнинга без включения в соответствующие реестры может, согласно закону, повлечь за собой уменьшение максимальной присоединенной мощности вплоть до полного отсоединения энергопринимающих устройств от электросети.

Майнеры обязаны предоставлять в уполномоченный правительством орган информацию о полученной в результате майнинга цифровой валюте. Этот орган, в свою очередь, будет передавать сведения Росфинмониторингу и Банку России. Адреса-идентификаторы также должны предоставляться по запросам Росфинмониторинга, ФСБ, ФНС и Росимущества.

Не очень понятен запрет на рекламу криптовалют и предложение их неограниченному кругу лиц, который начал действовать сразу после вступления закона в силу. Если майнинг легален, то почему нельзя рекламировать продажу производимой предпринимателем продукции – криптовалюты?

«Хорошо, что Государственная Дума обратила внимание на майнинг и криптовалюты. Но многое зависит от дальнейших шагов. По сути, Центральный банк становится законодательной властью для данного вида деятельности. Для бизнеса это хорошо тем, что позволит быстро менять правила игры в соответствии с его нуждами. И если такие правила будут согласованы ЦБ с исполнительной властью на предмет ненарушения других законов, то можно быстро приступить к работе, не ожидая долгих дебатов на уровне Госдумы. Хотя у этой медали есть оборотная сторона – ЦБ может так же быстро запретить ваши игры, поскольку нет никаких гарантий продолжительности экспериментальных правовых режимов», – дал комментарий нашему изданию архитектор блокчейн-платформы Erachain Дмитрий Ермолаев.

Ведение майнинга без включения в соответствующие реестры может повлечь за собой уменьшение максимальной присоединенной мощности вплоть до полного отсоединения энергопринимающих устройств от электросети

Полный текст статьи читайте на www.iksmedia.ru

Моновендорный ЦОД или комплексный подход

Александр Барсков

Понимание сути и ценность комплексного решения для инженерной инфраструктуры ЦОДов меняются. Продуктовое наполнение остается актуальным, но все более важными становятся вопросы экспертизы и сервисов поставщика.

Для работы размещаемых в ЦОДах ИТ-систем инженерная инфраструктура должна обеспечивать три ключевых ресурса: технологическое пространство для размещения ИТ-оборудования, электроэнергию для его электропитания и охлаждение для отвода тепла. В инженерную инфраструктуру могут входить несколько десятков различных подсистем, но названные три – основные.

Ключевым элементом системы электропитания ЦОДа являются источники бесперебойного питания (ИБП), обеспечивающие «очистку» электричества и автономное электропитание в случае отключений в электросети (обычно в течение 5–10 мин). За это время установленные на площадке генераторы (как правило, дизельные) должны запуститься и выйти на рабочий режим. Кроме того, в системы электропитания входят такие элементы, как трансформаторы, щитовое оборудование, автоматы ввода резерва (АВР), шинопроводы и др.

Основу системы охлаждения ИТ-оборудования ЦОДа составляют кондиционеры разных типов, как правило, внутрирядные (устанавливаются в один ряд с ИТ-шкафами) и периметральные (размещаются по периметру машзала). Кондиционеры могут работать на фреоне или на воде. В первом случае снаружи здания обычно устанавливают конденсаторы, а во втором – водоохлаждающие машины (чиллеры). Также в состав классических систем охлаждения входят другие элементы: насосы, трубопроводы, оборудование хладоцентра и т.д. Существуют и иные технологические варианты охлаждения, например холодные стены, адиабатические, погружные системы и пр.

Что касается размещения ИТ-оборудования, то здесь главный элемент – серверный шкаф (стойка). В него обычно устанавливают блоки распределения питания (БРП, PDU), организаторы кабельного хозяйства и пр. Для повышения эффективности работы систем охлаждения используются различные системы изоляции воздушных потоков. Наиболее популярная – система изоляции коридоров. На ряде объектов применяют фальшполы, пространство под которыми можно задействовать для подачи воздуха или размещения трубопроводов системы охлаждения, укладки кабельной проводки и пр.

Если в проекте основные элементы перечисленных трех систем поставляет один производитель, то такой ЦОД принято было называть моновендорным. Этот во многом маркетинговый термин активно продвигался рядом зарубежных производителей, способных предоставить обозначенный набор продуктов. Однако с уходом этих компаний из России владельцы «моновендорных ЦОДов», построенных на их оборудовании, ощутили серьезные проблемы с техобслуживанием и поддержкой. В результате понятие моновендорности многими компаниями и организациями стало восприниматься негативно. Тем не менее плюсы такого подхода сохранились, и его реализация на оборудовании отечественных компаний, которые никуда из страны не денутся, имеет немало преимуществ.

Насколько в новых условиях потенциальные заказчики заинтересованы в получении всех основных продуктов для инженерной инфраструктуры ЦОДа от одного производителя? В чем плюсы и минусы такого подхода? Насколько важно «одно окно» для сервисного обслуживания оборудования? Как изменился подход к выбору производителей после ухода с российского рынка большинства западных вендоров?

Чтобы ответить на эти вопросы, агентство iKS-Consulting и компания Systeme Electric провели в первой половине 2024 г. исследование, в ходе которого были опрошены технические директора, руководители технических подразделений и ведущие эксперты, работа которых связана с построением и эксплуатацией инженерных систем ЦОДов. В основном респонденты эксплуатируют ЦОДы средней и большой емкости. Так, примерно у половины принявших участие в опросе общая емкость ЦОДов превышает 100 стоек, а у 17% – 1000 стоек.

При выборе производителей продуктов для инженерной инфраструктуры ЦОДа заказчик, конечно, учитывает множество параметров, как технических, так и экономических. Большую роль играет репутация вендора и опыт применения его решений в уже завершенных проектах (в самой организации или в схожих у других участников рынка), экспертиза собственных специалистов и пр. В данной работе исследовались в основном базовые принципы выбора числа производителей, а также изменение критериев выбора после ухода из России западных брендов.

Реализация моновендорного подхода на оборудовании отечественных компаний, которые никуда из страны не денутся, имеет немало преимуществ

Принципы выбора

Как показало исследование, примерно треть ЦОДов стремятся выбирать наилучшие продукты на рынке, и работа с большим числом производителей их не смущает (рис. 1). При этом более 60% опрошенных в проектах построения ЦОДов обычно задействуют продукты четырех и более вендоров (рис. 2).

Диаметрально противоположного подхода – получить максимальное число продуктов из одних рук, от одного вендора – придерживается четверть респондентов. Довольно много опрошенных разочарованы текущим состоянием рынка: несмотря на наличие большого числа поставщиков, они полагают, что на данный момент особого выбора на рынке нет, поэтому приходится брать то, что доступно.

Как можно описать базовые принципы выбора числа производителей решений для инженерной инфраструктуры ЦОДа? (можно выбрать несколько вариантов)

Рис. 1. ▶
Базовые принципы выбора производителей решений для инженерной инфраструктуры ЦОДа

Представитель одного из крупнейших коммерческих ЦОДов отметил, что его компания старается работать с одним вендором по каждой системе (система бесперебойного питания – один вендор, система охлаждения – другой и т.д.), но использовать при этом типовые отраслевые решения, чтобы оборудование не было уникальным и его всегда можно было заменить оборудованием другого производителя. Вполне разумный подход в условиях турбулентности рынка.

Главным недостатком использования в инженерной инфраструктуре продуктов многих вендоров респонденты считают необходимость поддерживать так же много ЗИПов – на это указали почти 76% опрошенных. Примерно половина жалуются на плохую совместимость продуктов разных производителей, столько же – на необходимость ведения большого числа сервисных контрактов. 37,9% указали, что при возникновении проблем в инфраструктуре, в которой установлено оборудование большого числа производителей, трудно найти ответственного. Также к недостаткам данного подхода респонденты отнесли сложности мониторинга и конфигурирования.

Продукты скольких вендоров вы обычно используете в проектах построения инженерной инфраструктуры ЦОДов?

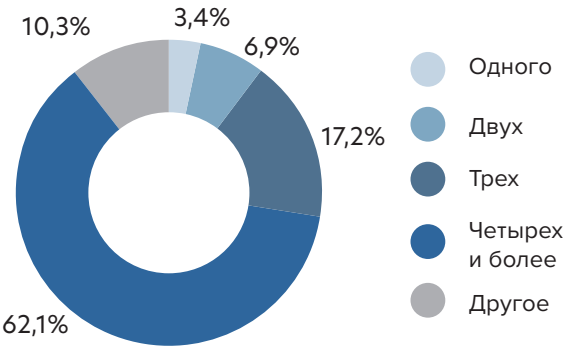


Рис. 2. ▶
Продукция какого числа вендоров обычно используется в проектах построения инженерной инфраструктуры ЦОДов

Основные же преимущества работы с одним вендором – хорошая совместимость продуктов (это отметили 48% респондентов), оптимизация ценового предложения в рамках комплексного решения (45%), а также «одно окно» при обслуживании и ремонте оборудования (41%). Хорошая совместимость позволяет существенно экономить на интеграции. Интеграция разношерстных продуктов разных вендоров в единую систему стоит недешево, что нивелирует возможную экономию на цене отдельных продуктов. Кроме того, дешевые продукты обладают ограниченными возможностями интеграции, поэтому из них часто невозможно построить действительно эффективное полное решение.

Примерно 38% отметили такое преимущество работы с одним вендором, как синхронизация сроков поставки. Она позволяет устанавливать оборудование на место сразу по поступлении на объект и экономить на том, что не нужно организовывать его длительное хранение.

После ухода из России большинства западных производителей инженерного оборудования для ЦОДов в 2022 г. потенциальные заказчики стали уделять больше внимания «глубине» присутствия вендора в стране. Почти 80% отметили то, что для них существенно выросла значимость наличия у компании-производителя офиса и складов (в том числе с ЗИПом) в России, а также квалифицированного персонала для инсталляции и эксплуатации продуктов (табл. 1). Данный критерий по своей важности обогнал даже российский статус производителя. Это и понятно: нахождение компании в российской юрисдикции еще не означает наличия у нее достаточной квалификации и опыта для поддержки оборудования.

Для ЦОДов всегда было крайне важно, чтобы производитель имел успешный опыт инсталляции и эксплуатации предлагаемых продуктов на других объектах. Значимость этого критерия вы-

Как изменился подход к выбору производителей для инженерной инфраструктуры ЦОДа после ухода с российского рынка большинства западных вендоров?

Критерий	Этот критерий для нас не имеет значения	Значимость этого критерия не изменилась	Значимость этого критерия существенно выросла
Это должен быть российский производитель – компания, которая находится в российской юрисдикции	37,9%	24,1%	37,9%
Производитель должен иметь в России офис, склады (в том числе с ЗИПом), квалифицированный персонал для инсталляции и эксплуатации продуктов	0	20,7%	79,3%
Производитель должен иметь успешный опыт инсталляции и эксплуатации предлагаемых продуктов в других ЦОДах в РФ	0	48,3%	51,7%
Мы должны иметь возможность проводить проверку (тестирование) продукции еще на заводе	20,7%	51,7%	27,6%
Оборудование производителя должно присутствовать в реестре Минпромторга	41,4%	31,0%	27,6%

▲ Табл. 1. Значимость различных критериев выбора производителей для инженерной инфраструктуры ЦОДа после ухода с рынка западных вендоров

росла для 51,7% респондентов. Однако надо понимать, что «старожилов» на рынке сейчас почти не осталось, работают в основном новые компании, поэтому наличие опыта инсталляции следует относить, скорее, к их специалистам, нежели к конкретным моделям продуктов.

Отметим, что для большой (41,4%) доли респондентов присутствие оборудования производителя в реестре Минпромторга не имеет значения. Однако почти для трети опрошенных ЦОДов значимость этого критерия выросла. Столько же участников опроса стали уделять больше внимания возможности проводить тестирование продукции еще на заводе – это особенно важно для новых продуктов, у которых пока нет истории успешного применения.

Чем комплексное отличается от моновендорного

Выше уже говорилось о том, что под моновендорным ЦОДом принято понимать объект, в котором три основные системы инженерной инфраструктуры (электропитание, охлаждение и средства размещения ИТ-оборудования) поставлены одним производителем. Однако после ухода из России основных мировых поставщиков «моновендорных ЦОДов» этот термин стал использоваться реже. Как показало исследование, заказчикам становится важнее не продуктовая, а сервисная составляющая, и они предпочитают говорить о комплексном решении (подходе). Именно предоставление вендором полного набора услуг на всех основных этапах жизненного цикла ЦОДа – от концепции до модернизации – респонденты считают главным критерием комплексности решения. На это указали 44,8% опрошенных (рис. 3).

На второе место в понятии комплексности респонденты ставят способность вендора предоставить различные варианты решения задач. Другими словами, специалисты такого поставщика должны иметь экспертизу по технологически разным вариантам решения поставленной заказчиком задачи – с необходимой продуктовой поддержкой.

Унификацию используемых изделий, которая упрощает эксплуатацию и материально-техническое обеспечение проектов, опрошенные называют наиболее важным преимуществом комплексного решения – его отметили 82,8% (учитывалась суммарная доля респондентов, поставивших этому критерию 4 и 5 баллов, табл. 2). На втором и третьем ме-

Что для вас означает понятие «комплексное решение для инженерной инфраструктуры ЦОДа»? Выберите все подходящие варианты

Рис. 3. Понятие «комплексное решение для инженерной инфраструктуры ЦОДа» ▼

Какие составляющие комплексного инфраструктурного решения для вас важны? Оцените значимость каждого из предложенных вариантов по пятибалльной системе: от 1 (не имеет значения) до 5 (очень важно)

	1	2	3	4	5
Предоставление всех основных продуктов «из одних рук»	10,3%	17,2%	34,5%	17,2%	20,7%
Ответственность за все решение в целом	0	0	20,7%	27,6%	51,7%
Комплексная сервисная поддержка	3,4%	3,4%	17,2%	24,1%	51,7%
Заранее реализованная интеграция продуктов	3,4%	6,9%	17,2%	41,4%	31,0%
Унификация для эксплуатации и материально-технического обеспечения	0	0	17,2%	34,5%	48,3%

▲ Табл. 2. Значимость составляющих комплексного инфраструктурного решения

стах – ответственность за все решение в целом (79,3%) и комплексная сервисная поддержка (75,8%). Собственно предоставление основных продуктов из одних рук (37,9%) оказалось только на пятом (последнем из предложенных вариантов) месте. Так что наличие «толстого каталога продуктов» должно быть поддержано экспертизой и набором сервисов.

Поскольку заказчики рассчитывают, что поставщик комплексного решения возьмет на себя ответственность на все решение, неудивительно, что они также ожидают от него готовности работать с оборудованием других производителей. Классический пример – производитель ИБП занимается интеграцией в общую систему бесперебойного и гарантированного электропитания ДГУ другого вендора (кстати, ДГУ будет всегда другого вендора – нам неизвестны производители, выпускающие и ИБП, и ДГУ). В ходе такой интеграции важно оптимально подобрать время автономной работы от АКБ, мощность ДГУ и пр.

Выполнение производителем – поставщиком комплексного решения работы по интеграции в единую систему продуктов других вендоров важно примерно для 80% респондентов. Примерно столько же надеются, что он поможет изменить проект в случае перехода на оборудование другого вендора. Это особенно актуально последние год-два в связи с кардинальным пересмотром заказчиками своих вендор-листов.

Сервис на всех стадиях

Как уже было показано, комплексная сервисная поддержка – одно из важнейших преимуществ комплексного решения. При этом сервисы «от производителя» важны не только на этапах инсталляции и эксплуатации, но и на других этапах жизненного цикла ЦОДа (табл. 3).

Так, на этапе планирования эксперты производителя могут привлекаться для аудита площадки, разработки концепции будущего объекта, оценки бюджета проекта и других задач. Это особенно важно, если учесть текущую ситуацию на российском рынке инженерного оборудования для ЦОДов. Когда идет кардинальная смена поставщиков и продуктов, заказчик может просто не знать особенности нового оборудования, ориентируясь на то, которое он использовал ранее и которое уже стало недоступным. Также на этапе планирования важна способность производителя предложить несколько разных вариантов технических решений, чтобы выбрать оптимальный для конкретной задачи. Понятно, что для этого он должен иметь экспертизу по разным технологиям, подкрепленную соответствующим продуктовым портфелем.

Сервисы производителя на этапе инсталляция понятны: это шеф-монтаж или монтаж под ключ, пусконаладочные работы (ПНР), обучение специалистов заказчика и др. При подготовке к эксплуатации помощь производителя нужна для разработки методик обслуживания оборудования и процедур эксплуатации. На этапе эксплуатации заказчики ожидают от производителя сервисного обслуживания оборудования с четко установленным SLA, управления ЗИПом и др. Для таких критически важных объектов, как ЦОДы, необходимо максимально оперативное восстановление штатного состояния систем в случае сбоев или аварий. Производи-

Насколько вами востребованы сервисы вендора на следующих основных этапах жизненного цикла ЦОДа? Оцените по пятибалльной системе: от 1 (нет необходимости) до 5 (абсолютно необходимы)

Этап жизненного цикла ЦОДа	1	2	3	4	5
Планирование	6,9%	3,4%	24,1%	37,9%	27,6%
Проектирование	6,9%	13,8%	10,3%	13,8%	55,2%
Инсталляция, включая ПНР	3,4%	0	13,8%	13,8%	69,0%
Эксплуатация	10,3%	6,9%	24,1%	24,1%	34,5%
Оптимизация и модернизация	6,9%	3,4%	20,7%	24,1%	44,8%

▲ Табл. 3.
Востребованность сервисов вендора на основных этапах жизненного цикла ЦОДа

тель должен разработать соответствующие процедуры и подкрепить их положениями в SLA.

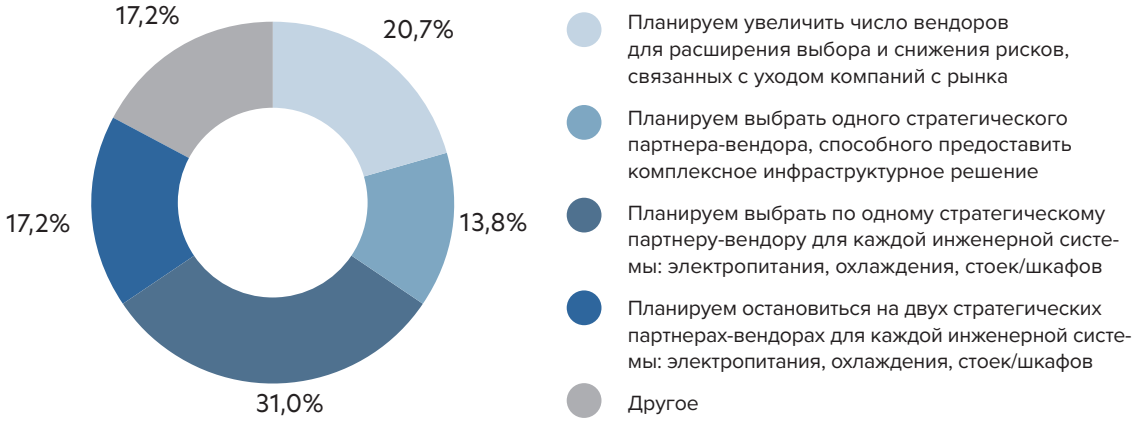
Как показал опрос (см. табл. 3), высок спрос на сервисы производителя и на этапах оптимизации и модернизации объектов. К работам по оптимизации можно отнести аудит объектов, добавление новых функций и цифровизацию оборудования, замену устаревших узлов или продление срока их службы. При модернизации обычно проводят плановую замену оборудования, в том числе в рамках контрактов поэтапной замены, а также комплексные работы по модернизации. Наконец, ответственный производитель должен предложить свои услуги и на финальной стадии, стадии вывода оборудования из эксплуатации. Эти услуги предусматривают, например, утилизацию аккумуляторных батарей или модулей ИБП.

Планы и выводы

Большая часть опрошенных (45%) планируют выбрать одного стратегического партнера-вендора либо для всего комплексного инфраструктурного решения, либо для каждой инженерной системы (электропитание, охлаждение, стойки/шкафы). Примерно 17% намерены остановиться на двух стратегических партнерах-вендорах для каждой инженерной системы (рис. 4).

Но все же турбулентность рынка ощущается: каждая пятая компания планирует увеличить число вендоров для расширения выбора и снижения рисков, связанных с уходом компаний с рынка. Представители ряда компаний отметили, что вообще не строят никаких планов, поскольку «все меняется каждый день». ИКС

Каковы ваши планы изменения политики работы с вендорами?



◀ Рис. 4.
Планы изменения политики работы с вендорами

ДКС: если предлагать, то производить самим!

В сентябре 2024 г. компания ДКС открыла две новые производственные линии на территории своего технопарка в Твери.

Получив в 2023 г. престижную премию DC Awards в номинации «Вендор решений для ЦОДов с самым высоким рыночным потенциалом», компания ДКС успешно этот потенциал реализует. Причем, как настоящий производитель, делает ставку на собственное производство.

В сентябре 2024 г. компания запустила в работу две новые производственные линии: по выпуску автоматических электрических выключателей и ИТ-шкафов. Производство автоматов организовано в новом корпусе площадью свыше 17 тыс. кв. м, который был построен всего за год.

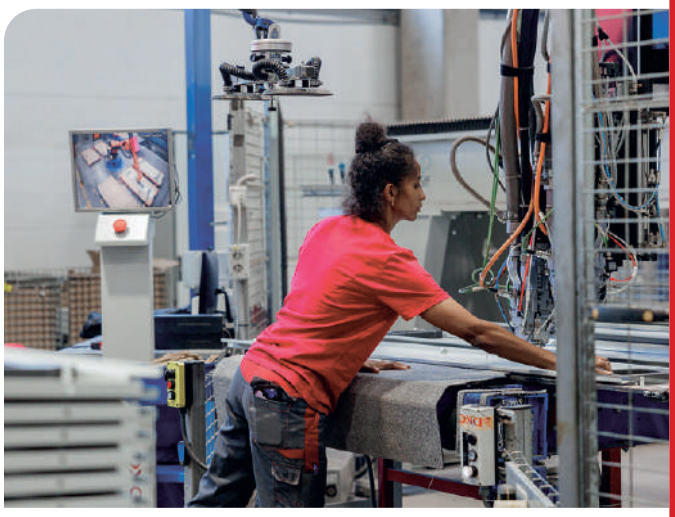
Как рассказал на открытии производства Дмитрий Колпашников, генеральный директор ДКС, в течение следующих двух лет цеха этого корпуса заполнятся новейшим технологическим оборудованием, на котором будут выпускаться низковольтная аппаратура самого высокого класса, мощные ИБП, в том числе модульные, зарядные устройства для автомобилей, решения для преобразования и хранения солнечной энергии, оборудование автоматизации. Кроме того, в корпусе будут развернуты современная лаборатория для испытаний и тестирования и научно-технический центр, который займется исследованиями в области новых технологий и разработками новых продуктов.

Дмитрий Колпашников,
генеральный директор компании ДКС

Будущее нашей экономики зависит от того, насколько эффективно мы сможем обрабатывать и использовать данные. Россия – один из мировых лидеров в области цифровизации, но отстает в развитии собственных решений для цифровой инфраструктуры. Очень важно, чтобы мы были технологически независимы от других стран, чтобы производили не только материалы, но и оборудование.

Шкафы ДКС начала выпускать еще в 2008 г., но до недавнего времени шкафы и стойки для ИТ-оборудования изготавливались как варианты общего конструктива (вместе с силовыми шкафами и шкафами для систем автоматизации) и в относительно небольшом количестве – 500–700 шкафов в квартал.

Однако в 2022 г. ряд партнеров компании, крупные цодостроители, обратились с просьбой сделать шкаф, который «просит рынок». Тогда же было принято решение об организации отдельного производства ИТ-шкафов. И вот в сентябре 2024 г. заработал цех, способный ежеквартально выпускать 3–3,5 тыс. шкафов, как стандартных 19-дюймовых, так и соответствующих стандарту OCP.



Испытания показали, что шкафы ДКС способны выдерживать нагрузку в 1,5 т, что соответствует самым строгим требованиям. Выпускаемые шкафы имеют ряд уникальных особенностей: в частности, благодаря использованию для дверей специального, более тягучего металла необходимая жесткость при высокой степени перфорации (82%) обеспечивается без специальных ребер жесткости.

По словам Дениса Горяченкова, руководителя отдела телекоммуникационных проектов ДКС, разработанный конструктив позволяет изготавливать шкафы высотой до 56U, а изделия 54U уже выпускаются и очень востребованы в связи с тенденцией к увеличению плотности ИТ-оборудования. Наличие собственной покрасочной камеры дает возможность окрашивать шкафы как в типовые цвета (черный и серый), так и в любые другие. К примеру, один заказчик уже заказал синие шкафы.

В портфеле решений ДКС для ЦОДов – производимые в Твери шинопроводы, фальшполы, ГРЩ, весь набор кабеленесущих систем. Также в России выпускаются ячейки среднего напряжения, силовые трансформаторы, структурированные кабельные системы (СКС). Пока часть ключевых продуктов привозится из-за границы, например, ИБП изготавливаются на заводе ДКС в Италии, но локализация их производства в России – в ближайших планах компании. В отделе цифровых решений много инженеров, программистов, электронщиков, схемотехников, которые активно наращивают компетенции, в том числе в области ИБП. Также идет разработка системы мониторинга и управления ЦОДами, которую ДКС планирует представить в 2025 г. Ведь философия компании: если что-то предлагать, то производить самим!

Виртуализация сетей: время облаков

Николай Носов

Виртуализация сетей и их предоставление по сервисной модели – перспективное направление развития облачных сервисов дата-центров.

Сеть для облака

Сначала договоримся о терминах: облако – это пул ресурсов для облачных вычислений, к основным характеристикам которых, согласно определению Национального института стандартов и технологий США, относятся: самообслуживание по требованию; универсальный доступ по сети; возможность объединения ресурсов; эластичность; учет потребления.

Реализация этих характеристик невозможна без гибкой и автоматически настраиваемой сети, отвечающей ряду специфических требований:

1. Обеспечение взаимодействия «всех со всеми», поскольку приложения, поддерживающие работу тех или иных сервисов, могут быть локализованы в любой точке ЦОДа.
2. Способность обслуживать большое число пользователей, находящихся в различных сегментах сети.
3. Обеспечение возможности работы приложений на любых серверах независимо от их физического расположения.
4. Возможность перемещения виртуальных машин (VM) между хостами, расположенными как внутри одного ЦОДа, так и в разных ЦОДах. При этом для некоторых технологий, например VMware vMotion, хосты должны находиться в одном L2-домене.
5. Поддержка управления большим количеством виртуальных и физических устройств в сети.
6. Способность обрабатывать огромное количество MAC-адресов и справляться с большими размерами MAC-таблиц, так как на одном физическом сервере могут находиться десятки виртуальных машин с уникальными MAC-адресами, а количество серверов в крупных ЦОДах измеряется тысячами.

Первое требование отражается в физической архитектуре сети. В отличие от трехуровневых систем, которые распространены в офисах и небольших корпоративных ЦОДах, в коммерческих ЦОДах, фокусирующихся на предоставлении облачных услуг, данные передаются преимущественно между серверами (горизонтальное направление, или «запад – восток»), а не от терминального устройства пользователя-человека к серверу и обратно (вертикальное, или «север – юг»). При этом задержки передачи сигнала критичны, что заставляет минимизировать количество промежуточных узлов сети. Это обусловило широкое применение в высокоскоростных сетях дата-центров двухуровневой архитектуры spine – leaf (технология Clos). Для обеспечения связи между отдельными модулями (pods) в машзале, между машзалами и даже ЦОДами добавляется еще один слой коммутаторов (super spine). При подключении к ним коммутаторов уровня spine используется тот же подход, что и уровнем ниже (рис. 1).

Оверлейные сети

Необходимость обслуживать большое количество пользователей ограничивает применение VLAN, ведь их число в сети не может превышать 4096 и крупное облако на таком числе изолированных сетей не построишь. Требование отсутствия привязки виртуальных машин к их физическому расположению обусловливает применение работающих на уровнях L3 оверлейных сетей (GRE, MPLS VPN, VXLAN, GENEVE), имеющих возможность передавать пакеты через каналы с разными протоколами канального уровня (рис. 2).

В облаках, построенных на базе Ethernet, часто используется протокол VXLAN (Virtual Extensible LAN, виртуальная расширяемая локальная сеть). VXLAN – это туннельный протокол, который инкапсулирует кадры Ethernet уровня L2 в UDP-пакеты уровня L4, позволяя создавать виртуализированные подсети уровня L2, охватывающие сети уровня L3. Каждая сегментированная подсеть имеет уникальный сетевой идентификатор VXLAN (VNI), число которых может достигать 16 млн – вполне достаточно для облака.

Транспортный протокол TCP, на котором построен интернет, хорош при ненадежных каналах связи, но он медленнее, чем UDP. В ЦОДе каналы надежные, а скорость имеет первоочеред-

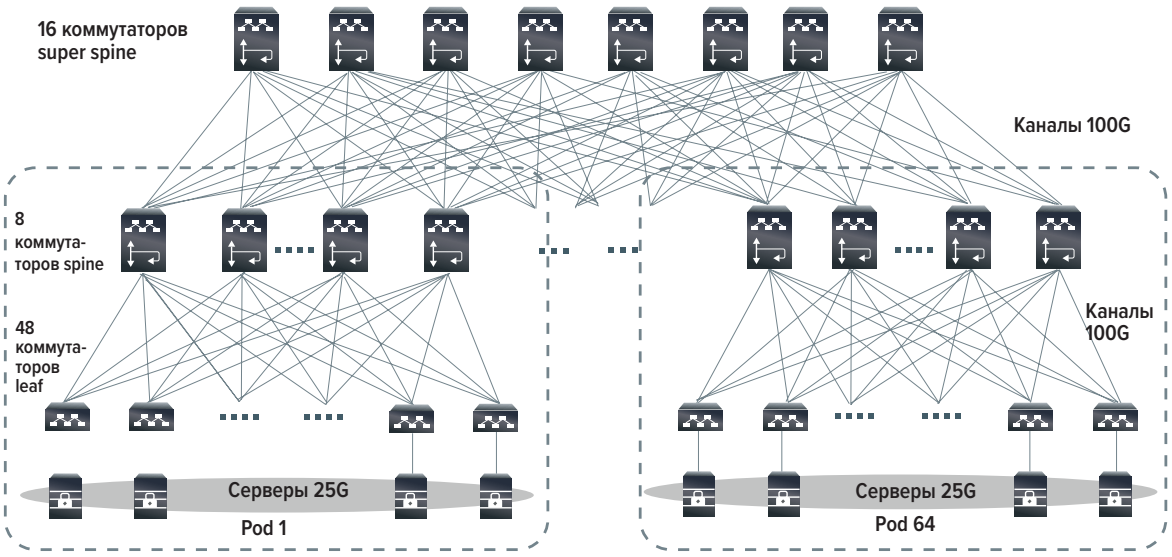


Рис. 1. Горизонтальная архитектура с объединением нескольких подов (дата-центров)

Источник: Cisco

ное значение, поэтому на транспортном уровне VXLAN используется протокол UDP (рис. 3).

С помощью VXLAN можно объединить в локальную сеть виртуальные машины, находящиеся в разных сетях (рис. 4) и даже ЦОДах.

Серверная виртуализация и реализация оверлейных сетей

На базе физической ИТ-инфраструктуры в ЦОДе облачный провайдер разворачивает облачную платформу, включающую в себя средства виртуализации серверов, хранилищ данных и сетей, систему управления, учета потребления ресурсов и биллинга.

Основа облачной платформы – серверная виртуализация, когда на физическом сервере (ноде, хосте) устанавливается гипервизор (чаще всего ESXi или KVM), делящий ресурсы центрального процессора и память между виртуальными машинами. Каждой виртуальной машине и каждому из контейнеров, которые можно рассматривать как упрощенные виртуальные машины с общей операционной системой, назначаются свои IP- и MAC-адреса. По этим адресам развернутый на хосте виртуальный многоуровневый коммутатор (в решениях VMware – vSwitch, в OpenStack – OVS) осуществляет маршрутизацию. К «внешним портам» виртуального коммутатора подключаются физические сетевые карты хоста.

Далее пакеты попадают на коммутатор уровня доступа, который в ЦОДе чаще всего расположен вверху стойки (Top of Rack, ToR).

При этом оверлейные сети могут создаваться как на аппаратных коммутаторах доступа, так и на виртуальных коммутаторах (роутерах) хостов (рис. 5). В российских дата-центрах чаще используются виртуальные, поскольку они более гибкие и вендоронезависи-

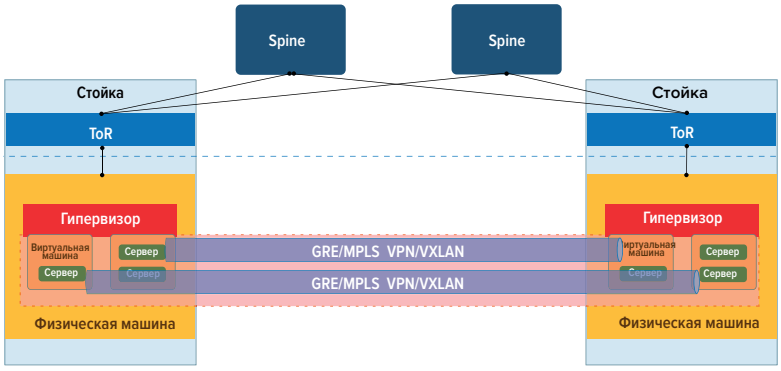


Рис. 2. Оверлейные сети, связывающие виртуальные машины на нодах в разных стойках

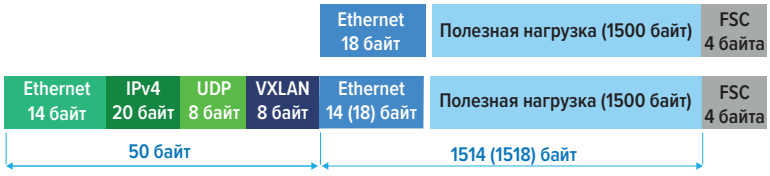
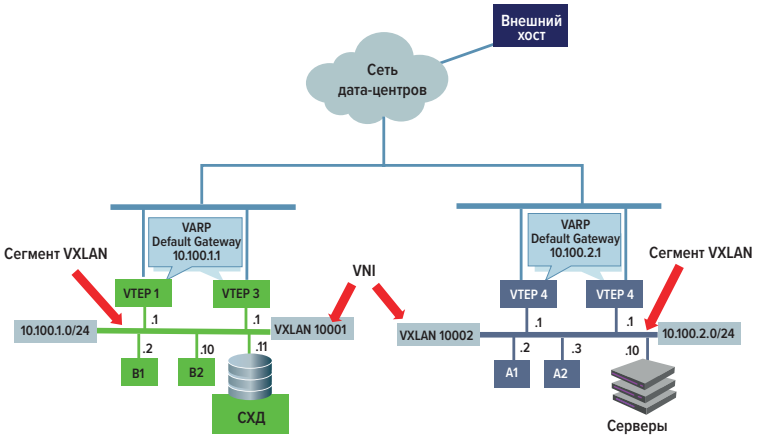
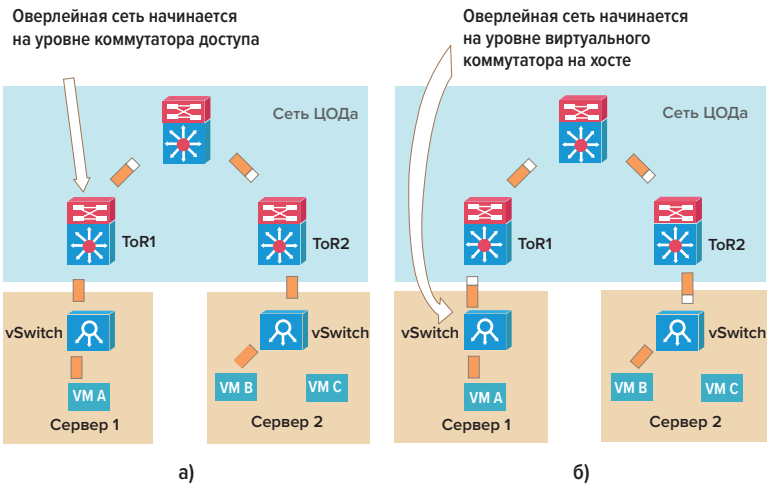


Рис. 3. Структура кадра VXLAN



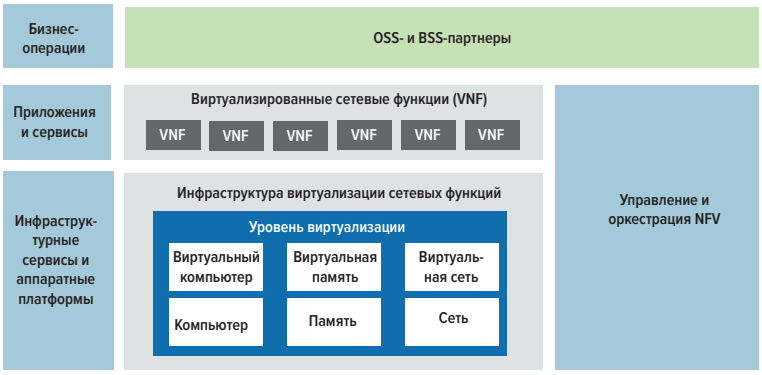
Источник: Arista

Рис. 4. Объединение локальных сетей с помощью VXLAN



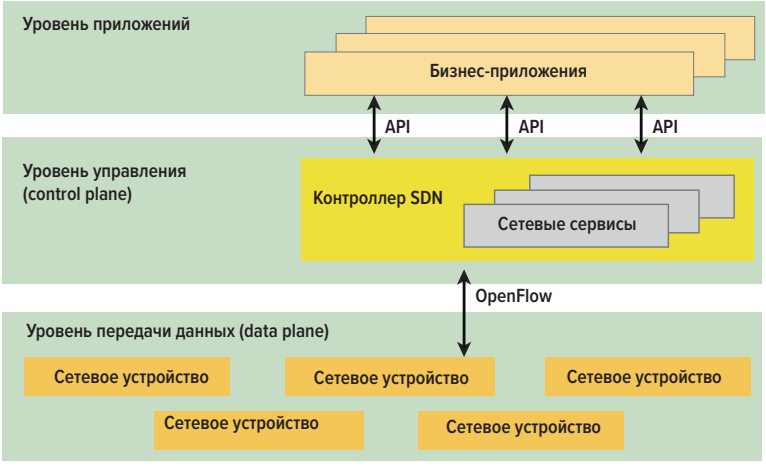
Источник: CBS

▲ Рис. 5. Архитектура оверлейной сети, построенной на коммутаторах доступа (а) и на виртуальных роутерах (б)



Источник: Juniper

▲ Рис. 6. Архитектура NFV



Источник: Open Networking Foundation

▲ Рис. 7. Архитектура сети SDN

мые, что особенно важно в условиях санкций и импортозамещения.

Виртуализация сетевых функций

Любой аппаратный шлюз, коммутатор или маршрутизатор можно рассматривать как компьютер, оптимизированный для выполнения специализированных задач. Сетевое устройство можно эмулировать, развернув соответствующий образ на виртуальной машине. Такой подход лежит в основе концепции виртуализации сетевых функций, предложенной Европейским институтом телекоммуникационных стандартов еще в 2012 г.

Принципы разработанного для телекома подхода с успехом применяются и в облачных средах. На стандартизированных вычислительных узлах (контейнерах, виртуальных машинах, виртуальных сетях и системах хранения) – инфраструктуре виртуализации сетевых функций (Network Functions Virtualization, NFV) – создаются виртуализированные сетевые функции (Virtualized Network Function, VNF), т.е. программные реализации сетевых функций (брандмауэры, балансировщики нагрузки, шлюзы широкополосных сетей). Вместо отдельных аппаратных решений для каждой сетевой функции используются программно настраиваемые VNF, которые могут включать несколько виртуальных машин, серверы, коммутаторы, хранилища и даже инфраструктуру облачных вычислений. Оркестрацию, масштабирование и балансировку нагрузки между отдельными VNF осуществляет система управления NFV (рис. 6).

Программно определяемые сети

Таким образом, у нас есть технологии построения виртуальных машин, виртуальных сетей и виртуальных сетевых устройств. Для построения облачной платформы не хватает механизма гибкого управления сетями для автоматизированной переконфигурации связей между всеми этими объектами.

На помощь приходит технология программно определяемых сетей (рис. 7, 8) – разделения уровней управления (Control Plane) и передачи данных (Data Plane).

Задача уровня Data Plane – быстрая пересылка трафика с входных интерфейсов в выходные в соответствии с таблицами маршрутизации. Здесь главное – скорость передачи, а медленно думающие «мозги» располагаются на уровне Control Plane, отвечающем за контроль состояния сети и заполнения таблицы маршрутизации. На этом уровне работает контроллер SDN, выполняющий функции управления, аналитики и оркестрации сети.

Управление сетью в облаке

Разделение уровней передачи данных и уровня управления – основа построения сети в облаке, что можно проиллюстрировать на примере открытой облачной платформы OpenStack (рис. 9).

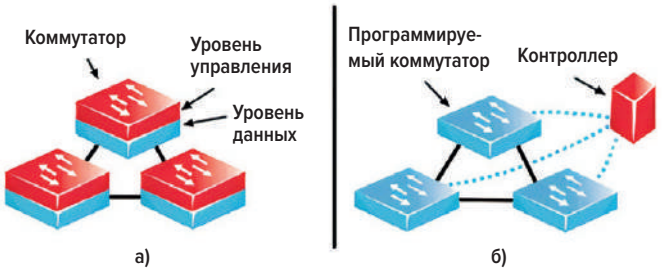
Для развертывания облачной платформы нужно минимум два сервера (хоста, ноды). Один – для вычислительных ресурсов (Compute Node), другой – для блока управления (Controller Node). На Controller Node в принципе может находиться и узел с сетевыми устройствами, но на практике, чтобы не терять в производительности, их размещают на отдельных серверах – Network Node.

На серверах Compute Node с помощью гипервизора создаются виртуальные машины. Для подключения виртуальной машины к физической сети на сервере запускается виртуальный роутер (vSwitch в решениях VMware, OVS – в OpenStack), подключающий на уровне L2 виртуальную машину к физической сетевой карте (которых для резервирования должно быть минимум две на каждый сервер). К этому виртуальному коммутатору подключаются (через эмулирующие порты для внутренней сети интеграционного моста br-int) и другие виртуальные машины пользователя, запущенные на этой ноде, образуя его собственную виртуальную локальную вычислительную сеть (VLAN).

Внутренние соединения имеют более высокую пропускную способность по сравнению с соединениями через коммутаторы за пределами хоста, что надо учитывать клиенту при развертывании виртуальной инфраструктуры. Например, использовать скоростную внутреннюю виртуальную сеть, подключая виртуальную машину через виртуальный коммутатор с базой данных, находящейся на этом же хосте.

Мост br-tun в виртуальном роутере сервера отвечает за создание туннелей между виртуальными машинами и сетевыми устройствами на Network Node и оверлейных сетей (VXLAN), связывающих виртуальные машины на разных хостах (Compute Node). Управление виртуальным роутером (OVS) осуществляется с помощью установленного на хосте агента (Neutron Open vSwitch Agent), который загружает получаемые по сети управления (еще как минимум две сетевые карты на каждый сервер) настройки и таблицы маршрутизации от расположенного на Controller Node контроллера сети (Neutron API Server).

В OpenStack на Controller Node в роли SDN-контроллера выступает Neutron API Server, поддерживающий сетевые топологии, включая развертывание и настройку сетей и подсетей, создание, обновление и удаление портов. Для оптимизации трафика в оверлейных сетях VXLAN и GRE используется специальный плагин (ML2 Plugin OVS Mecriver).



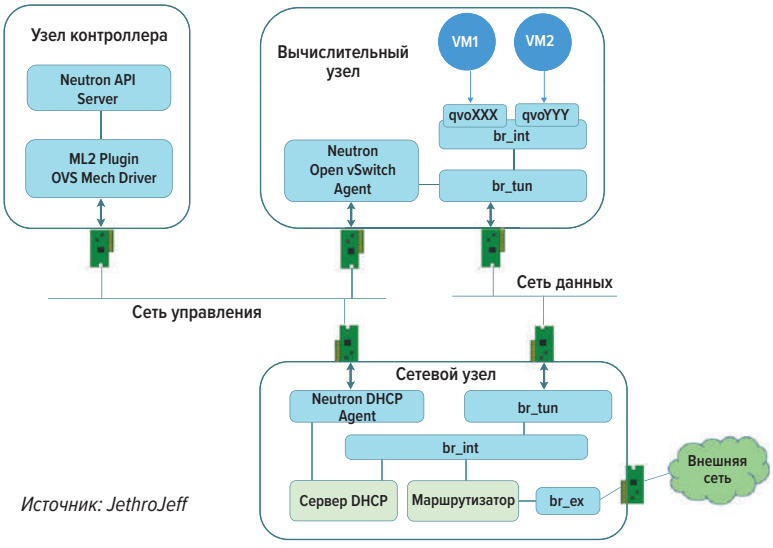
▲ **Рис. 8.** **Традиционная (а) и программно определяемая (б) сетевая инфраструктура**

Ресурсоемкие сетевые сервисы разворачивают на выделенных нодах – сетевых узлах (Network Node). В числе таких сервисов – серверы DHCP, отвечающие за выделение IP-адреса в сети TCP/IP, и виртуальные роутеры. На Network Node располагается и мост к внешним сетям (br-ex). Дублирование сетевых функций на разных нодах позволяет легко переносить нагрузку между нодами и сохранять работоспособность виртуальной сети пользователя при отказе физических серверов.

На основе OpenStack создан ряд российских облачных платформ, в том числе VK и Selectel, и на этой же базе отечественные компании дорабатывают решения для виртуализации сети.

«Наши продукты можно рассматривать как некий комплексный аналог VNF. Они представляют собой облачные сервисы, состоящие из множества виртуальных машин, состав которых может динамически меняться, например, при увеличении нагрузки. Все продукты – исключительно программные. В основе нашей облачной платформы лежит OpenStack, но не «ванильный», а доработанный для высокопроизводительных масштабируемых облачных вычис-

Рис. 9. **Архитектура OpenStack**▼



Источник: JethroJeff

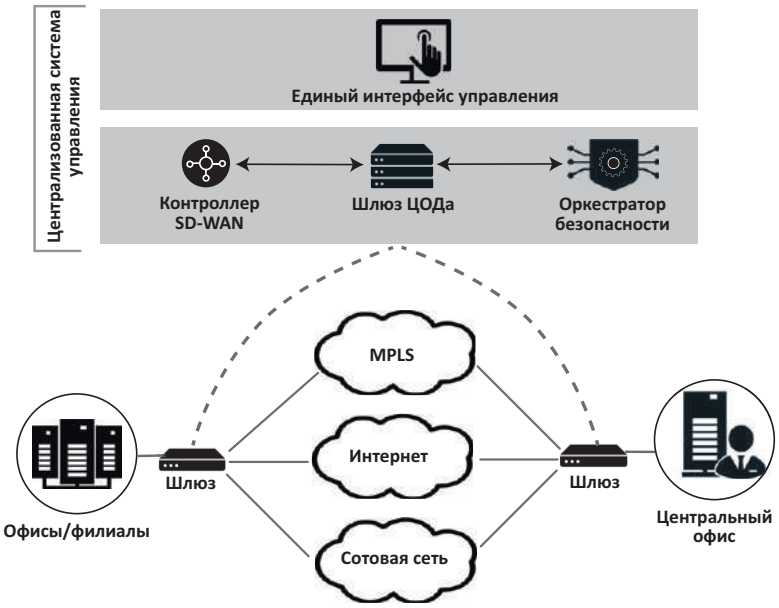


Рис. 10. Архитектура SD-WAN

лений. Использование open source позволило быстро запуститься, хотя параллельно мы работаем над собственным SDN-решением, переход на которое планируем осуществить в ближайшее время. Решение позволит объединить множество облачных платформ и обеспечить взаимодействие между ними», – дал комментарий нашему изданию главный архитектор сетевой инфраструктуры компании CloudX Сергей Колесников.

Виртуальные внешние сети

Принцип разделения сети на уровень передачи данных и уровень управления применим и к внешним сетям, обеспечивающим доступ к ЦОДам. В решениях SD-WAN в качестве каналов выступают сотовая сеть, сеть MPLS и VPN-туннели через интернет, а узел контроллера, управляющий уровнем передачи данных, может находиться в облаке или на одной из площадок клиента (рис. 10). При этом одновременно решаются вопросы резервирования каналов, балансировки нагрузки между ними и оптимальной маршрутизации в зависимости от типа трафика.

Используя виртуализацию (например, платформу VMware NSX) для внешних сетей и дата-центров, можно создать единый центр управления сетями в распределенной виртуальной инфраструктуре – виртуальную облачную сеть, связывающую дата-центры головных компаний, отделений, edge-ЦОДы, публичные и частные облака и даже устройства интернета вещей (рис. 11).

Рис. 11. Виртуальная облачная сеть под управлением NSX ▼

Источник: VMware

Сеть как облачный сервис

Как и виртуальные машины, сети можно создавать и уничтожать по требованию, например, кратковременно предоставляя доступ к ЦОДу с архивом или для переноса нагрузки или расширения канала до резервного ЦОДа в случае аварии на основном. Виртуализация сетевых функций позволяет гибко управлять трафиком и обеспечивать оптимальную маршрутизацию, предоставлять сетевые соединения и канал требуемой пропускной способности по запросу. Появляется возможность предоставления сети как облачного сервиса (Network as a Service, NaaS).

NaaS включает в себя предоставление из облака сервисов как локальных сетей (LAN as a Service, LANaaS), в том числе управление сетями и обеспечение их безопасности, так и внешних сетей (WAN as a Service, WANaaS), в том числе сервисы мультиплексирования WAN (MPLS) и SD-WAN.

Все эти услуги набирают популярность в мире. По оценкам Market.us, мировой рынок NaaS вырастет с $14,6 млрд в 2023 г. до $115,5 млрд в 2032 г.

Российский рынок решений NaaS отстает от мирового. По оценкам экспертов, отставание составляет два-три года. На карте российского ПО виртуализации уже появились вендоры, предлагающие решения SD-WAN, и их количество увеличивается. Правда, в реестре отечественного ПО пока нет решений российских вендоров SDN, зато много облачных платформ, использующих open source-решения для виртуализации сети, в основном на основе OVS.

Виртуализация сетей и их использование по сервисной модели привлекает мало внимания, но это перспективный рынок. Развитие отечественных ИТ в целом повторяет развитие мировых, поэтому можно полагать, что объем услуг NaaS в России будет расти. ИКС

ЦОД-2024. Инфраструктура для облака

Российский облачный рынок продолжает стремительно развиваться, формируя спрос на стойкую к санкциям инфраструктуру. Новым драйвером может стать искусственный интеллект.

Николай Носов

Рост рынка

Уход западных вендоров и введенные санкции положительно сказались на российском рынке коммерческих ЦОДов, который, как сообщил на 19-м ежегодном форуме «ЦОД» ведущий консультант iKS-Consulting Станислав Мирин, увеличится в 2024 г. на 17%. Причем средний рост в 2022–2024 гг. составит 18,9%, по сравнению с 10,4% среднего роста в 2018–2021 гг. (рис. 1).

Существенный вклад в возросший спрос на услуги коммерческих ЦОДов внесли облачные сервисы, доля которых постоянно увеличивается и почти в полтора раза превысила долю преобладавших до 2020 г. услуг colocation (рис. 2).

К основным драйверам роста рынка коммерческих ЦОДов – цифровой трансформации предприятий, переходу на цифровые сервисы, постоянному росту объема хранимых и обрабатываемых данных – добавились импортозамещение цифровых услуг и рост российских облачных сервисов. В условиях нестабильности и сложностей с оплатой и поставкой ИТ-оборудования привлекательность сервисной модели потребления ИТ-ресурсов в глазах клиентов повышается. А давление регуляторов, особенно на владельцев значимых объектов КИИ, заставляет компании искать быстрые варианты импортозамещения, и часто выходом становится перенос инфраструктуры в облако.

Нас бьют, а мы крепчаем

Санкционное давление усиливается. В мае 2024 г. подписки на свои облачные сервисы для российского бизнеса начала блокировать Microsoft. Лишив монетизации на YouTube, а затем выгнав из рекламной сети AdSense, выдавливает россиян из своих облаков Google.

С 12 сентября США запретили предоставлять облачные услуги планирования ресурсов предприятия (ERP), управления взаимоотношениями с клиентами (CRM), бизнес-аналитики (BI), управления цепочками поставок (SCM), корпоративного хранилища данных (EDW), управления техническим обслуживанием (CMMS), а также проектами и жизненным циклом продукта (PLM) «любому лицу, находящемуся на территории России».

В этих условиях резко возрос спрос на услуги российских облачных провайдеров. В том числе тех, которые предоставляют привычное для российских пользователей западное ПО. Например, Cloud4Y, которая, по словам технического пресейла компании Дианы Тусовой, вполне легально обеспечивает возможность работы по сервисной модели с западным ПО из своего дата-центра в Турции.

Перспективным выглядит вынос российскими провайдерами части облачной инфраструктуры в ЦОДы, расположенные в дружественных странах, скажем, в Казахстане и Узбекистане. Сотрудничество взаимовыгодное – страны получают налоги, рабочие места и повышают экспертизу своих специалистов, а облачные провайдеры могут легально предлагать российским клиентам подсанкционный софт.

Искусство резьбы по OpenStack

Использование ПО нейтральных стран тоже сопряжено с рисками, что продемонстрировал израильский конструктор сайтов Wix, заявивший,

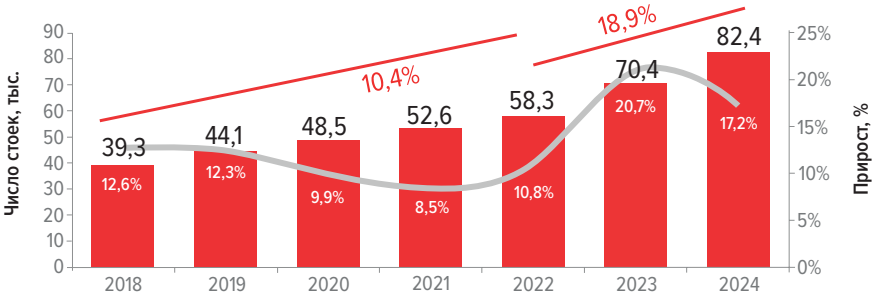


Рис. 1. Динамика роста коммерческих ЦОДов в России

Источник: iKS-Consulting

что с 12 сентября заблокирует аккаунты российских пользователей. Проживающие в России пользователи больше не смогут получить доступ к своему аккаунту, а созданные ими на платформе Wix сайты будут сняты с публикации. Компания «любезно» предложила россиянам перенести их на другой хостинг, по сути – за пару дней сохранить, что получится, а потом в авральном порядке создать новый сайт, ведь прежний работоспособен только на израильской платформе. Удар, который может похоронить бизнес многих тесно связанных с интернетом компаний.

Не дает стопроцентной гарантии и использование ПО, разработанного в России, – к санкциям присоединилась и проданная в 2021 г. канадцам российская компания Ecwid, чьи конструкторы интернет-магазинов активно использовались малым и средним бизнесом. Возможно, для российских компаний, имеющих продукты в реестре российского ПО, стоит рассмотреть ограничения на продажу за рубеж без согласования с регулятором, например, Минцифры?

Но все же использование услуг российского облачного провайдера и российского ПО – самый надежный вариант. Тем более что в области виртуализации и облачных платформ предложений много. Спасает open source, прежде всего гипервизор KVM, системы управления OVirt и облачная платформа OpenStack, лежащие в основе большинства российских решений. Отечественные вендоры, не мудрствуя лукаво, делают тюнинг программ с открытым исходным кодом, «подпиливая» их под свои нужды, а то и просто берут «ванильный» вариант. Подход нормальный, рабочий, так же поступают и крупные зарубежные компании, например, Red Hat. Главное, чтобы в компании было достаточное число квалифицированных программистов, способных развивать продукт и оказывать полноценную поддержку клиенту. Правда, с этим у компаний, ранее не занимавшихся системами виртуализации, нередко возникают проблемы.

Снизить требования к сопровождающему решения персоналу можно, используя программно-аппаратные комплексы (ПАК) с «подогнанной» к поставляемому «железу» системой виртуализации. По этому пути пошла компания «Гравитон», представившая на конференции «ЦОД» гиперконвергентное решение HELIUS. В ПАК, созданный на серверах «Гравитона», входит доработанная под аппаратное обеспечение классическая связка OpenStack и Ceph. Запрос на такие решения есть, поскольку с 1 сентября вступил в силу запрет Правительства РФ на использование на значимых объектах критической информационной инфраструктуры приобретенных после этой даты ПАК иностранного производства.

Экосистемы российских продуктов

Создание собственных экосистем и коллаборация с другими игроками рынка – логичный путь развития занимающихся импортозамещением российских компаний. Причем экосистемы совместимых решений расширяются. «Мы продаем не только программное обеспечение, но и ПАК. Мы тесно сотрудничаем с российскими производителями, в том числе с «Гравитоном», Qtech и OpenYard, с продукцией которых наши решения совместимы и могут успешно работать», – сообщил генеральный директор vStack Евгений Карпов. Стоит вспомнить и реализацию гиперконвергентной платформы vStack в составе ПАК на аппаратных решениях российской компании GAGAR>N.

Компания vStack существенно расширила линейку продуктов виртуализации – за последний год в реестре отечественного ПО появилось хранилище vStack SDS, которое способно работать и в связке с решениями VMware, проходят регистрацию vStack OS, vStack Backup и vStack VDI. Биллинг и панель самообслуживания уже имеются, так что клиенты получают полноценную облачную платформу, которую можно использовать для развертывания не только частных, но и публичных облаков.

ЦОДы для ИИ

«Требования российских заказчиков сильно меняются. Исторически мы – производитель се-

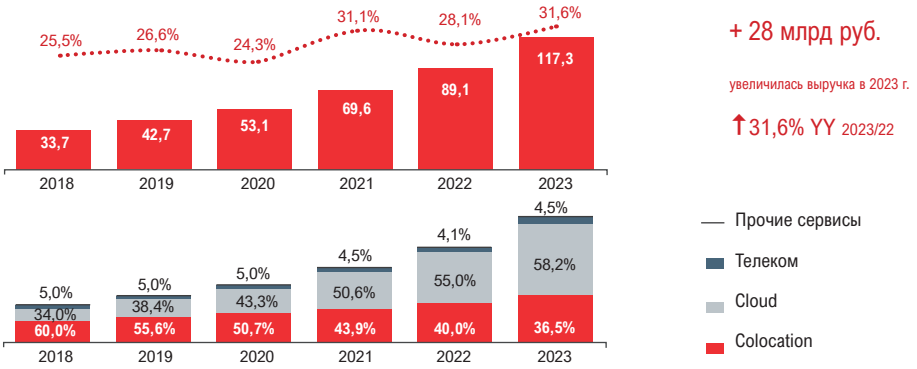


Рис. 2. Объем (млрд руб.) и структура рынка ЦОДов ▶

Источник: iKS-Consulting

тевого оборудования. Но последние два года основной объем запросов связан с серверами с GPU и системами искусственного интеллекта», – отметил менеджер по развитию бизнеса Qtech Александр Кудряшов. Компания откликнулась на требования рынка и начала выпускать серверы с GPU, в которых важна не мощность центрального процессора, а количество поддерживаемых графических плат. Действительно, спрос на оборудование для ИИ стремительно растет, и темпы роста, по прогнозам iKS-Consulting, будут только увеличиваться. Не будем дискутировать, нужно ли одному из немногих российских вендоров сетевого оборудования распылять силы и самому делать все, вплоть до серверов, СХД, написания ПО программно определяемой инфраструктуры и изготовления серверных стоек.

Другой аспект спроса на ИИ-системы – энергопотребление. Например, в одну из моделей серверной платформы Qtech можно установить до 10 графических карт. Если брать поддерживаемый этой моделью Nvidia Tesla GPU мощностью 300 Вт, то энергопотребление GPU только одной четырехюнитовой корзины составит 3 кВт, а максимальная нагрузка на стойку 48U приблизится к 40 кВт. Что уж говорить о современных зарубежных решениях для ИИ с энергопотреблением более 10 кВт на сервер.

Такое количество тепла трудно снимать только воздушным охлаждением, но эти задачи могут решаться инновационными методами. Так, IXcellerate предлагает использовать в ЦОДе воздушное охлаждение для традиционных стоек и гибридное – и воздухом, и водой – для высоконагруженных, средней мощностью 40 кВт. «Но это один и тот же ЦОД. Все зависит от того, с каким оборудованием к нам придет клиент», – пояснил технический директор компании Сергей Вышемирский. Если у клиента системы с прямым жидкостным охлаждением, то дата-центр обеспечит отвод тепла даже от стоек с потреблением 100 кВт, в то время как 10-киловаттные стойки будут охлаждаться воздухом.

Доклад вызвал большой интерес – в зале не хватило мест для всех желающих. Тема острая, срок эксплуатации ЦОДа длительный, и еще на этапе проекта потребности клиентов надо просчитывать минимум на 10 лет вперед. Самые мощные ускорители на базе GPU уже сегодня потребляют до 1 кВт. Ожидается, что к концу текущего десятилетия этот показатель достигнет 2 кВт. Если ИИ будет активно внедряться в бизнес-процессы, потребуется много высоконагруженных стоек.

Хотя в плане использования коммерческих ЦОДов для обучения моделей всё неоднозначно. В настоящее время лидирующие на отечественном рынке ИИ компании задействуют собственные дата-центры. Своими суперкомпьютерами обзавелись «Яндекс», Сбер и МТС. Неочевидно, что им потребуются высоконагруженные стойки в коммерческих ЦОДах. Также на базе своих ЦОДов они могут предлагать услуги обучения моделей и высокопроизводительных вычислений по облачной модели. С другой стороны, мощностей постоянно не хватает, а наличие собственных корпоративных ЦОДов не мешает крупным заказчикам использовать услуги коммерческих дата-центров.

Облако и государство

На цодостроение и развитие облачных услуг большое влияние оказывает государство. С 1 января 2025 г. запускается в промышленную эксплуатацию «Гособлако». В нем смогут работать не только федеральные, но и региональные и даже муниципальные органы власти. Государство оценило преимущества сервисной модели и всячески способствует ее распространению. «Когда “Гособлако” только формировалось, перед федеральными органами власти “повесили морковку” – финансирование эксплуатации их информационных систем через Минцифры. Теперь предлагается то же самое сделать с регионами», – заявил директор по взаимодействию с органами государственной власти и организациями «Ростелеком-ЦОД» Дмитрий Панышев.

Минцифры собрало запросы регионов в отношении вычислительных мощностей. Эксперт уверен, что уже к концу года появятся регионы-пилоты, потребляющие облачные ресурсы за федеральный счет, причем не только по модели IaaS. Все это положительно скажется на развитии облачных услуг в России.

Главное – доверие

Те российские компании, которые и в условиях санкций умудряются поддерживать работоспособность продуктов ушедших с рынка западных вендоров, по мнению экспертов, приложат все усилия, чтобы продолжать их использование. Но уже многие полностью перешли на отечественные продукты, и даже в гипотетическом варианте снятия санкций, скажем, в 2025 г. и возвращения западных вендоров в Россию они вряд ли снова встанут в ряды их пользователей. Потеряно главное – доверие, причем не только на российском рынке, но и на рынках многих развивающихся стран, которых наш пример заставил задуматься об обеспечении технологической независимости, в том числе в сфере облачных платформ.

Новым российским игрокам придется нелегко, на рынке останутся только сильнейшие, но отечественные облака выживут и будут развиваться – в этом у экспертов сомнений нет. ИКС

ЦОД для ИИ. IXcellerate уже строит

IXcellerate готовит к запуску первый, пока экспериментальный машзал с технологией прямого жидкостного охлаждения. В планах – объект на 100 МВт. Подробности рассказывает технический директор компании Сергей Вышемирский.

– Начнем с самого простого (и одновременно очень сложного) вопроса: что такое ЦОД для искусственного интеллекта?

– Общепринятого определения нет. Как и обычный ЦОД, это здание с комплексом инженерно-технических систем, но спроектированное и построенное под иные требования, главным образом в расчете на другую энергетическую плотность. Сегодня в наших ЦОДах этот показатель в новых контрактах 2024 г. в среднем составляет 12 кВт (на стойку) и выше, но для систем ИИ необходимы стойки на 40–45 кВт и более.

Понятно, что ЦОД для таких стоек должен обеспечить соответствующую энергетическую мощность. Например, один модуль ИИ (ряд из 12–16 стоек) – это уже почти 800 кВт только ИТ-мощности. В одном зале может быть, скажем, 20 таких рядов – очень высокая нагрузка. ЦОД для ИИ – это энергетический гигант, который отличается от обычных дата-центров тем, что может, во-первых, обеспечить такую мощность для ИТ-оборудования и, во-вторых, охладить его. Традиционные системы охлаждения не проектировались под такие параметры.

В обычных ЦОДах, конечно, можно попробовать развернуть ИИ-системы: распределить по площади, по этажам, чтобы в каждой стойке было по одному высоконагруженному ИИ-серверу. Так сейчас и делают в большинстве дата-центров в России. Громадные затраты на СКС, большие задержки сигналов, что по меньшей мере неэффективно, да и не всегда работает. В ЦОДе для ИИ стойки стоят кучно: чем ближе друг к другу, тем короче соединительные линии, тем быстрее вычисления.

Поэтому ЦОД для ИИ – это очень высокая плотность. А чтобы получить максимальную плотность – и весь мир это понял, – надо переходить на прямое жидкостное охлаждение серверов.

– Эта технология исключает традиционное охлаждение воздухом?

– Сразу скажу, что мы пока не рассматриваем погружное (иммерсивное) охлаждение. Там еще хватает проблем, в том числе с обеспечением циркуляции охлаждающей жидкости (как правило, негорючего масла) в емкости, куда погружают серверы.

А вот у контактного охлаждения перспективы хорошие. Но в этом случае охлаждающие пластины накладываются только на наиболее горячие компоненты – процессоры и видеокарты, а блоки питания, материнские платы и другие элементы должны охлаждаться воздухом. Скажем, с 50-киловаттной стойки с прямым жидкостным охлаждением до 8 кВт тепла надо снимать воздухом.

Пионеры в области жидкостного охлаждения – создатели суперкомпьютеров – в свое время хорошо это поняли. Так, для одного из наиболее производительных суперкомпьютеров России изначально сделали только жидкостное охлаждение, воздушное не предусмотрели. Когда запустили и поняли, что ИТ-системы перегреваются, добавили обычное фреоновое охлаждение.

– Какие именно решения для поддержки высоконагруженных стоек разрабатываются или уже внедрены в ЦОДах IXcellerate?

– Начали мы с совершенствования систем воздушного охлаждения. Замечу, что если у обычных серверов разница в температуре воздуха на входе и выходе составляет обычно 6–10°С, максимум 12°С, то у высоконагруженных – 16–20°С. Традиционные системы охлаждения такую разницу просто не вытянут.

Наша R&D-команда совместно с технологическими партнерами – ведущими производителями систем охлаждения – разработала универсальное охлаждающее оборудование, которое способно работать с любыми серверами: с разницей как 6°С, так и 20°С. Нужные характеристики достигаются главным образом за счет увеличения площади теплообмена. На заводе для нас все изготовили, протестировали, все прекрасно работает. На наших новых площадках в Южном кампусе это решение уже внедрено и позволяет снимать до 50 кВт тепла со стойки.

Кстати, чиллеры, подающие теплоноситель на охлаждающее оборудование, тоже доработали. Взяли за основу простое решение с винтовым компрессором и частотным преобразователем, что позволило избежать больших пусковых токов, и обеспечили чиллеру бесперебойное питание. Мы один из немногих ЦОДов в России, который для бесперебойного охлаждения вместо баков – аккумуляторов холода – использует АКБ и ИБП.

– 50 кВт на стойку – предел для воздушного охлаждения?

– На самом деле уже после 25–30 кВт доля энергии, которую потребляют вентиляторы, начинает быстро расти, а после 50 кВт охлаждать воздухом категорически неэффективно. Дальше – прямое жидкостное охлаждение.

Очень долго искали решение этой задачи. Ведь ставить две параллельные системы – воздушного и водяного ох-

лаждения – крайне невыгодно. Да и конструктивно разместить второй комплекс оборудования, проложить к каждой стойке еще по две (а для резервирования – по четыре) трубы зачастую просто нереально.

Выход нашли совместно с одним из наших технологических партнеров. Не нужно строить две параллельные системы. Разработали единую систему, которая обеспечивает и воздушное, и жидкостное охлаждение. Причем блоки распределения жидкости (CDU) и контроллеры устанавливаются не в каждой стойке, а по одному на группу стоек. Система обеспечивает отведение со стойки до 100 кВт тепла. Сейчас строим экспериментальный зал на 1100 кВт общей ИТ-мощности (12–16 стоек). По плану запустим в эксплуатацию в начале следующего года.

Уже разработали концептуальный проект ЦОДа на 100 МВт с поддержкой систем прямого жидкостного охлаждения.

– Много ли заказчиков на 100-киловаттные стойки?

– Этот вопрос мы сами себе постоянно задаем. Изначально мы сделали концепт проекта на 100 МВт. Потом немного притормозили, решили поэкспериментировать с небольшим залом, провести исследование рынка. Один, якорный, заказчик у нас есть. Еще минимум три компании хотят поставить свои стойки в нашем экспериментальном зале.

К тому же, пусть в 2024 г. это решение востребовано всего несколькими заказчиками. В 2025 г. их число несомненно увеличится, а в 2026-м – когда мы и должны активно строить наш 100-мегаваттный объект – спрос вырастет резко. И мы будем первыми, кто построит большой коммерческий ЦОД с прямым жидкостным охлаждением для систем ИИ. Собственно, лидер и должен работать на перспективу, формировать рынок.

– Про ЦОД для ИИ мы поговорили. А каковы перспективы использования ИИ для ЦОДа? Какие преимущества искусственный интеллект может дать в плане его эксплуатации?

– Дать искусственному интеллекту самому управлять ЦОДом – категорическое «нет». Но в помощь эксплуатации – однозначное «да».

Когда ты эксплуатируешь 8 тыс. стоек, у тебя более 150 клиентов, перед которыми ты несешь колоссальную ответственность, в том числе в виде штрафных санкций, важно минимизировать вероятность ошибок, связанных с человеческим фактором. В этом и призван помочь искусственный интеллект. Глобальных отказов у нас не было, но разные инциденты случались, и никогда они не были связаны с качеством оборудования, все проблемы обусловлены пресловутым человеческим фактором.

Приведу пример. 4 января 2024 г. случился блэкаут, весь Северо-Восточный округ столицы остался без электричества. Понятно, у нас одномоментно запустились десятки ДГУ, на пультах управления все заморгало и замигало, несколько сотен сообщений в одну секунду. Как выбрать наиболее важные? Ведь в дежурной службе всего семь человек. Искусственный интеллект в таких случаях помогает оперативно проанализировать все, отфильтровать второстепенные сообщения, обратить внимание на наиболее важные.

Другой момент – проактивное техобслуживание. Я за то, чтобы предупреждать поломки, а не ремонтировать, когда что-то уже сломалось. Системы с искусственным интеллектом способны отслеживать тенденции, приводящие впоследствии к сбоям.

Мы уже переходим на проактивность. Например, ежемесячно проводим анализ масла в ДГУ, смотрим, что происходит с дизелем (эта методика более 50 лет успешно практикуется в авиации). Если появляется медь, значит, проблема с цилиндрами, с подшипниками. Следующий шаг – ввести эти данные в ПО с искусственным интеллектом, который быстрее и точнее диагностирует проблему.

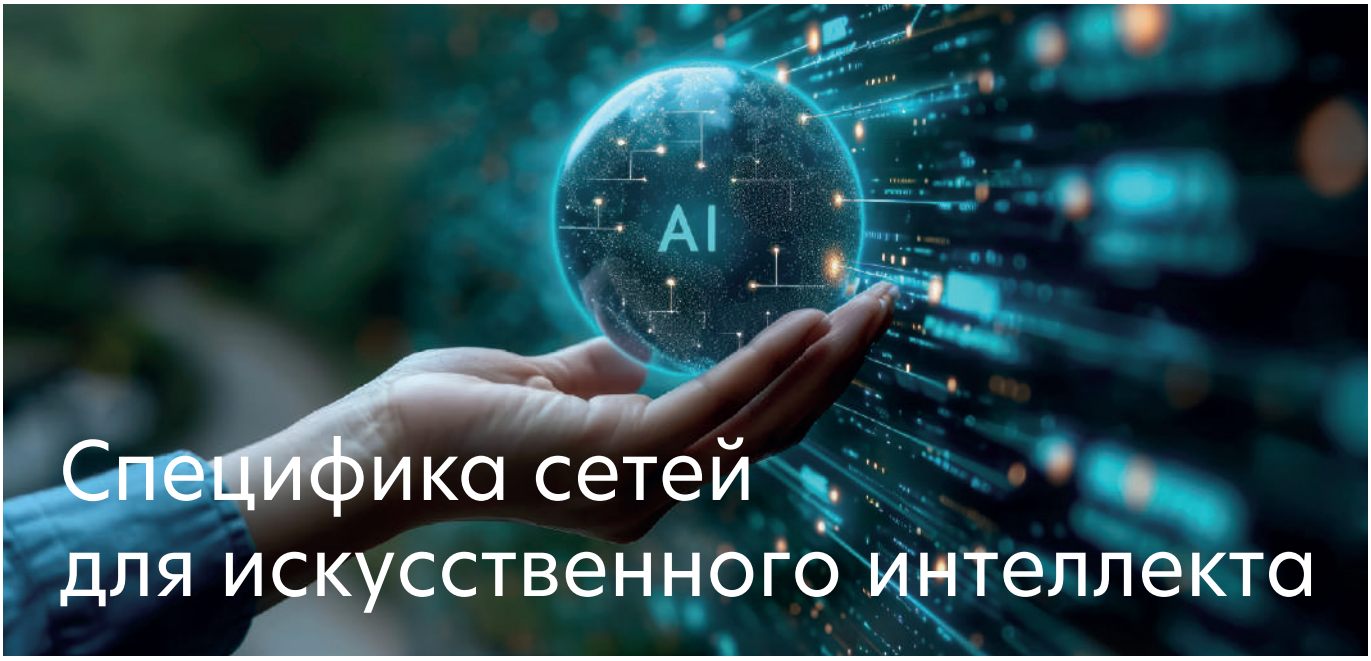
Сейчас переходим на новую систему управления эксплуатацией. Будем ее дорабатывать, опираясь на собственную экспертизу. В нее по максимуму внедрим элементы ИИ, чтобы система подсказывала службе эксплуатации, исключала ошибки, блокировала неверные действия. Планируем интеграцию с системой видеонаблюдения (которая будет «видеть», что происходит, и сообщать о нештатных ситуациях), со складскими системами, системами закупок (например, если со склада взяли ЗИП, чтобы резерв автоматически пополнялся) и т.д. Важный момент – интеграция с системой мониторинга, со средствами термодинамического моделирования, чтобы в случае фиксации перегрева в какой-либо точке машзала система управления сама подсказывала, что нужно делать. Наша цель – полностью исключить незапланированные остановки оборудования.

– Как ИИ изменит отрасль ЦОДов в целом?

– Отрасль, без сомнения, изменится. ИИ будет стремиться туда, где есть электричество, потому что ему нужно много энергии. Соответственно, огромные ЦОДы будут строиться в местах максимальной доступности электроэнергии. Но это не исключает развития небольших ЦОДов, обслуживающих локальные потребности. За счет близости к пользователям эти edge-ЦОДы обеспечат максимальную скорость реакции на их запросы.

Мы, хотя и работаем в Москве, тоже ориентируемся не на красивые площадки, а на те районы, где есть энергия. Еще в 2019 г. поняли, что ЦОДам для развития нужны огромные мощности. Поэтому выбрали для своего Южного кампуса Бирюлево – единственный район Москвы, где было в свободном доступе 300 МВт электроэнергии.

Мы будем двигаться в направлении инноваций. Для этого, помимо технологического сотрудничества с ведущими вендорами, важно развивать собственную экспертизу, взаимодействовать с научными кругами. Человеческий фактор – это риски при эксплуатации, но это и база для развития. Мы тесно сотрудничаем с НИУ «МЭИ», в частности, совместно разрабатываем решения, которые позволят увеличить эффективность работы вентиляторов в системах воздушного охлаждения (снизить потери воздушного тракта), а также теплообменники для жидкостного охлаждения серверов. Уверены, что все это позволит нам упрочить позиции технологического лидерства в российской отрасли ЦОДов.



Специфика сетей для искусственного интеллекта

Николай Носов

Учет особенностей задач искусственного интеллекта при построении сети вычислительного комплекса позволит повысить скорость обучения моделей. Но адекватные архитектурные решения пока не разработаны.

Требования к сети

Обучение моделей искусственного интеллекта строится на обработке большого объема данных, причем, как правило, чем больше данных, тем точнее будет работать модель. Данные загружаются в вычислительную систему, после чего оптимизированным перебором вариантов (скажем, методом градиентного спуска) в них начинается поиск связей и закономерностей. На уровне инфраструктуры ускорить вычисления можно путем повышения скорости обработки, например, увеличив число процессоров и их мощность, а также скорости передачи данных, за что отвечает сеть.

Машинное обучение – процесс цикличный и легко распараллеливаемый, что обусловливает широкое применение графических ускорителей (GPU). На сотнях, а то и тысячах ядер GPU одновременно обрабатывается огромный массив данных, разбитый на малые сегменты. По завершении цикла оценивается результат работы модели, проводится корректировка, и цикл повторяется до достижения приемлемого результата. Чем больше GPU, тем быстрее обучается модель ИИ.

Графические процессоры, обработав свои данные, делятся результатом со всеми другими графическими процессорами. Тут в повышении производительности системы начинает играть важную роль сеть. «Передача больших объемов данных от множества хостов ко всем остальным хостам предъявляет серьезные требования к сети вычислительной системы», – отметил на конференции IT Elements руководитель группы сетевых пресейлов компании «Инфосистемы Джет» Алексей Цемарков. Прежде всего сеть должна быстро, надежно и бережно передавать большие синхронизированные потоки данных, не допуская потерь. Кроме того, время передачи пакета должно быть постоянным, поскольку задержка даже одного пакета может существенно влиять на время выполнения задачи. Если на всех GPU цикл вычислений завершился и все начали обмениваться информацией со всеми, а из-за перегрузки канала или коллизий данные одного GPU задержались, то вычислительный кластер будет ждать, пока все процессоры не предоставят свои результаты. Еще одно требование к сети – равномерное распределение потоков и мониторинг узких мест. Чем больше сеть, тем труднее все эти требования выполнить, не говоря уже о том, что они плохо согласуются со ставшей практически стандартом технологией Ethernet.

Сетевая карта вместо CPU

В классической сети сетевые пакеты записываются в буфер ядра, затем CPU копирует их в буферы приложений. На этом теряется время. Учитывая, что в системах ИИ по сути выполняется одно приложение, процесс можно ускорить – передавать данные из памяти удаленного узла в локальную память инициатора запроса непосредственно сетевым контроллером без участия CPU. Такой подход обеспечивает технология удаленного прямого доступа к памяти (Remote Direct Memory Access, RDMA). При этом используются пары очередей, которые отобра-

жаются в областях памяти пользовательского пространства, а сетевая карта напрямую, минуя CPU и ОС, через сеть считывает/записывает данные в эти области.

Подход RDMA поддерживает технология InfiniBand, широко используемая в высокопроизводительных вычислениях и суперкомпьютерах, в том числе в пяти из первой десятки (на июнь 2024 г.) суперкомпьютеров рейтинга Top500 и в замыкающем тройку лидеров американском Eagle. Сеть InfiniBand используется и в большинстве российских суперкомпьютеров, например, в Christofari Сбера, базирующемся на GPU Nvidia DGX-2.

Сетевое оборудование, поддерживающее InfiniBand, дорогое и сильно зависит от вендора – компании Nvidia, которая купила ключевого разработчика технологии, компанию Mellanox. В условиях санкций для России перспективнее выглядит использование сетей Ethernet, тем более что производительность их значительно выросла и уже не кажутся экзотикой сетевые карты, обеспечивающие скорость до 400 Гбит/с.

Для работы RDMA поверх традиционных сетей Ethernet разработан протокол RoCE (RDMA over Converged Ethernet).

Первая версия (RoCE v1) работала на канальном (L2) уровне, осуществляя связь между любыми двумя хостами в одном и том же широковещательном домене Ethernet. Вторая версия протокола (RoCE v2) обеспечивает маршрутизацию пакетов и их передачу без потерь. Она улучшена включением в заголовок поля UDP/IP (рис. 1), поддерживает возможность работы в L3-сетях и сигнал явного уведомления о перегрузке (Explicit Congestion Notification, ECN).

Распределение нагрузки на каналы

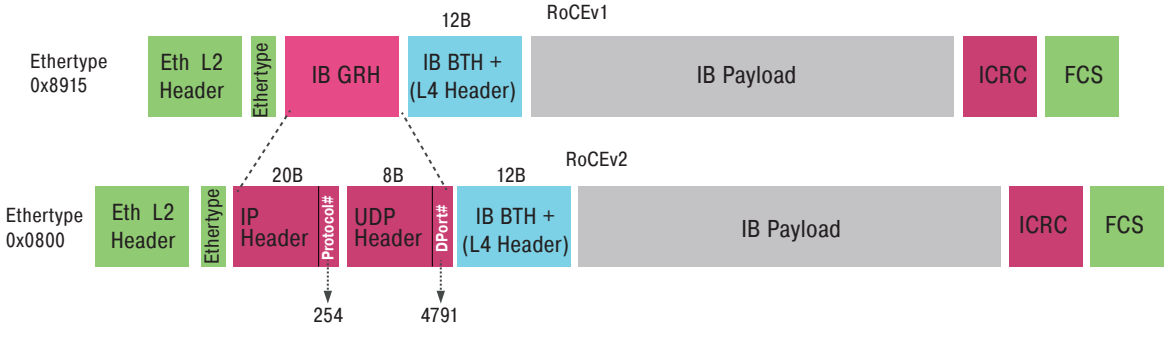
Цикл обработки данных может удлиниться из-за неправильного распределения нагрузки, когда пакеты стоят в очереди на обработку к одному хосту, в то время как остальные свободны. Для балансировки нагрузки на каналы в сетевых фабриках применяется технология ECMP (Equal Cost Multi-Path), позволяющая одновременно задействовать для передачи данных несколько равнозначных маршрутов, что повышает эффективность и надежность передачи сетевого трафика. В этом случае набор из пяти полей в заголовке пакета – IP-адрес источника (ip-src), IP-адрес назначения (ip-dst), номер порта источника (port-src), номер порта назначения (port-dst), протокол (например, TCP или UDP) – служит уникальным идентификатором соединения в сети. Обычно в ЦОДе работает много приложений, и порты используются разные, что дает возможность балансировать трафик по соединениям. Однако в сетях для ИИ порт назначения в основном один и тот же, поскольку, как уже говорилось, в вычислительной системе работает по сути одно приложение. Стандартных методов балансировки по портам недостаточно, и это приводит к перегрузке отдельных каналов.

Вендоры по-разному подходят к проблеме. Одни применяют отдельные контроллеры для анализа загруженности, другие пытаются заложить алгоритмы балансировки на уровне чипов. Единого стандартизированного подхода нет, что усложняет жизнь разработчикам вычислительных комплексов для ИИ.

Еще одна проблема сетей ИИ – Incast, т.е. перегрузка, возникающая в сети, когда множество уже выполнивших вычисления хостов одновременно пытаются отправить большой объем информации на один хост. Ему не хватает пропускной способности для обработки, но трафик терять нельзя.

И здесь предлагаются разные методы, ни один из которых не решает проблему полностью. Самый простой – использование больших буферов памяти на коммутаторах или сетевых картах. Но при современных скоростях этого недостаточно, поскольку буферы быстро переполняются поступающими пакетами. Другой метод состоит в том, чтобы при переполнении канала на хост источника или вышестоящий коммутатор посылать сигнал «пауза» или снижать скорость передачи пакетов. Делать это можно, например, при помощи механизма ECN (рис. 2), позволяющего сетевым устройствам уведомлять отправителей о перегрузках в сети.

Сетевая карта источника, получив сигнал о переполнении канала, дает указание своему



◀ Рис. 1. Структура кадра Ethernet в протоколах RoCE версии 1 и 2

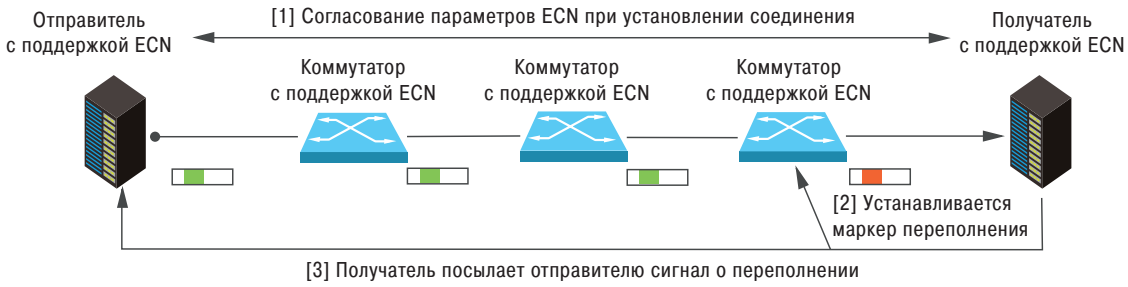


Рис. 2. ▶ Реализация механизма ECN

серверу о снижении скорости обработки. Ограничение метода – в том, что все устройства сети должны поддерживать ECN.

Нужен общий подход

В настоящее время ни для одной из описанных выше проблем нет всеобъемлющего и общепринятого решения. «Разброд и шатания. Каждый пытается решить проблемы по-своему, но на уровне индустрии они не закрыты. Нет готового дизайн-гайда – делай так, и будешь прав», – описывает текущее состояние рынка А. Цемарков. Чтобы навести порядок, год назад был создан консорциум UEC (Ultra Ethernet Consortium), в который вошли ведущие ИТ-компании, в том числе AMD, Arista, Broadcom, Cisco, Intel, Juniper, Huawei и Microsoft. И даже Nvidia, хотя и считает InfiniBand лучшим интерконнектом для ИИ-кластеров и является фактически единственным поставщиком данной технологии, в мае 2024 г. тоже присоединилась к консорциуму.

UEC будет определять протоколы, характеристики электрической и оптической связи, интерфейсы для прикладных программ и структуры данных в сети Ethernet для расширения или замены существующих каналов связи и транспортных протоколов.

Среди задач консорциума – повышение масштабируемости хостов от нескольких тысяч до миллиона, обеспечение автоматического контроля перегрузки сетей, чтобы коммутаторы и сетевые устройства могли сами «договориться» и уменьшить задержку до получения последнего пакета цикла обработки.

UEC Stack должен быть обратно совместим с существующим стеком, на транспортном уровне (L4) поддерживать синтаксис общения устройств для получения сквозной информации о происходящем в сети и выравнивания нагрузки.

К этому добавится шифрование «из коробки», повышающее безопасность сети. Среди планируемых новшеств – балансировка на уровне не потоков, а пакетов, причем с уходом от жесткого правила последовательной посылки фреймов. Правда, пока непонятно, как потом эти «распыленные» по разным каналам пакеты собирать. Разве что предоставлять инструкцию по сборке на конечном хосте.

Вопросов много, но можно надеяться, что подходы к построению сетей для ИИ удастся упорядочить, новые подходы внедрить и выработать если не стандарты, то хотя бы общие рекомендации. ИКС

Серверы для ИИ: что предлагают российские производители

Бум интереса к приложениям, использующим искусственный интеллект, привел к росту спроса на соответствующие серверы. Несмотря на сложности, связанные с зависимостью от иностранных комплектующих, российские производители смогли оперативно на него ответить.

Илья Бедердинов

Объем мирового рынка серверов для ИИ-приложений в 2023 г. составил, по данным Verified Market Research, $40,6 млрд, и ожидается, что к 2030 г. он увеличится до $166,6 млрд при среднегодовом росте 17,45% (рис. 1). Более высокий темп роста этого рынка – 34,46% – прогнозирует Market Research Future. По оценкам этой компании, рынок ИИ-серверов составлял $9,75 в 2022 г. и достигнет $188,35 в 2032 г. Прогнозы различаются, но основные драйверы те же – непрерывно повышающийся спрос на ИИ-приложения в разных отраслях и потребность в обработке данных в реальном времени.

Российские эксперты также фиксируют заметный рост спроса на серверное оборудование для проектов, связанных с ИИ. Причем, как отметили в компании GAGAR>N, речь в большинстве случаев идет не просто об исследованиях и перспективных разработках, а о серьезных коммерческих проектах в разных отраслях экономики, предполагающих реальную экономическую отдачу.

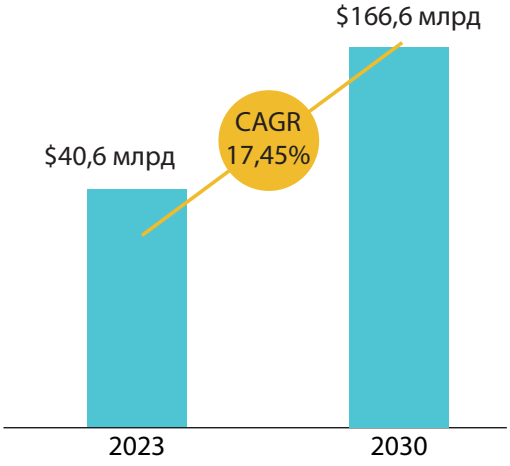
«Вплоть до 2023 г. запросов на серверы для ИИ было немного – в среднем мы выполняли два-три проекта в квартал. Сейчас же среди крупных компаний интерес к такому оборудованию увеличился в несколько раз. Есть спрос и со стороны небольших заказчиков – как правило, они выбирают GPU-серверы, которые хорошо масштабируются», – говорит Андрей Головских, руководитель направления серверного оборудования Crusader компании 3Logic Group.

Не GPU единым

Для обучения больших моделей, как правило, используются графические процессоры (Graphics Processing Unit, GPU), самым известным производителем которых является компания Nvidia. GPU специализируется на обработке графики и параллельных вычислениях. Его главная задача – одновременно обеспечивать визуальное воспроизведение, отрисовку графики и выполнение сложных вычислений. Это делает GPU оптимальным инструментом для трехмерной графики, виртуальной реальности, научной деятельности и многих других областей, где параллельная обработка данных имеет решающее значение.

Однако для ряда задач ИИ использовать графические ускорители необязательно, достаточно CPU новейших поколений. Так, по словам Александра Фильченкова, руководителя управления серверных и сетевых систем компании «Гравитон», ее серверы на базе процессоров общего назначения Intel Xeon Scalable 4-го и 5-го поколений успешно справляются с задачами для ИИ, в частности машинным обучением. Эти процессоры созданы с поддержкой ускорения ИИ в каждом ядре, что обеспечивает скачок в общей производительности, а также снижает совокупную стоимость владения.

Эксперт «Гравитона» обращает внимание на предстоящий выход процессора Intel Xeon 6-го поколения, производительность которого в расчете на 1 Вт должна быть в 2,6 раза выше, чем у предыдущих поколений. «С помощью ускорителей ИИ Gaudi 2 и Gaudi 3 Intel стремится сделать внедрение ИИ более доступным. Эти процессоры предназначены для ускорения выполнения рабочих нагрузок ИИ, особенно в области обучения и выводов генеративного ИИ, и составят конкуренцию решениям Nvidia», – считает А. Фильченков.



◀ Рис. 1. Мировой рынок серверов для приложений, использующих ИИ

Источник: Verified Market Research

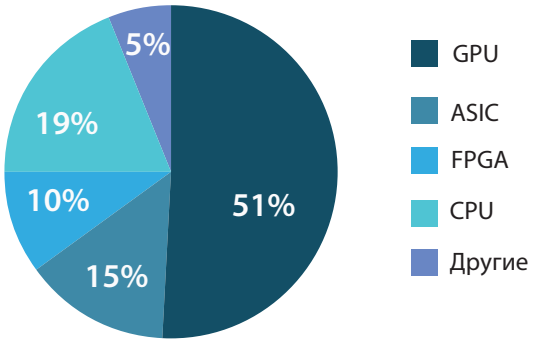


Рис. 2.
Доли рынка ИИ-серверов на основе разных вычислительных компонентов, 2023 ▶

Источник: Global Market Insights

Повышенное внимание поддержке ИИ-технологий уделяет и компания AMD, анонсировавшая технологию AMD Instinct AI и серверные процессоры AMD EPYC 5-го поколения. Их выпуск запланирован на второе полугодие 2024 г. По планам производителя, они будут отличаться высокой производительностью и эффективностью при работе с ИИ.

Помимо решений на основе GPU и CPU, для приложений на базе ИИ задействуются и другие типы серверов. Например, компания «Тринити» сообщила, что предлагает для этих задач серверы TPU и FPGA. TPU – Tensor Processing Unit – это специализированная интегральная схема (Application-Specific Integrated Circuit, ASIC) ускорителя ИИ, разработанная Google для машинного обучения нейронных сетей с использованием собственного ПО. Google начала применять TPU внутри компании в 2015 г., а в 2018 г. сделала их доступными для сторонних потребителей в рамках своей облачной инфраструктуры и предложила уменьшенную версию чипа для продажи. В мае 2024 г. компания анонсировала уже шестую версию – TPU v6.

FPGA (Field-Programmable Gate Array), или программируемая пользователем вентильная матрица – полупроводниковое устройство, которое может быть сконфигурировано уже после изготовления. Серверы с матрицами FPGA позволяют гибко настраивать вычислительные процессы под конкретные задачи ИИ.

На мировом рынке ИИ-серверов решения на базе GPU, по данным Global Market Insights, занимают чуть больше половины (рис. 2). На втором месте – ИИ-серверы с использованием CPU (почти 19% рынка), далее следуют устройства на базе ASIC (включая TPU) и FPGA.

Выбор сервера с определенным типом процессора для обучения нейросетей и работы с ними зависит не только от специфики решаемой задачи, но и от множества других факторов, таких как бюджет, требования к производительности, масштабируемости, доступные ресурсы. Ниже мы рассмотрим ряд решений, предлагаемых российскими производителями.

Crusader

Под маркой Crusader ИТ-дистрибьютор 3Logic Group предлагает серверы серии Squire HPC с поддержкой до восьми двухслотовых графических ускорителей с ОЗУ типа DDR5 4800/4400 объемом до 6 Тбайт. Топовая модель в портфеле компании, Crusader HPC Squire 4245R – двухпроцессорный сервер (на базе процессора 4-го поколения AMD EPYC 9004) с поддержкой графических ускорителей вплоть до моделей Nvidia Tesla Ada H100.

Сценарий применения таких серверов определяется потребностями заказчика. По словам А. Головских, оборудование компании используется в первую очередь для интеллектуального анализа данных и обработки естественного языка, в том числе виртуальных помощников и чат-ботов. Такие инсталляции составляют около 80%. На втором месте – задачи компьютерного зрения.

3Logic Group имеет собственные производственные линии, что обеспечивает поставку оборудования, точно соответствующего утвержденной спецификации.

DataPy

В портфеле продуктов DataPy представлено оборудование, предназначенное для высокопроизводительных вычислений, включая приложения на базе искусственного интеллекта. ИИ-серверы DataPy ориентированы на задачи обучения больших языковых моделей, рекомендательных систем, видеоаналитики, анализа данных и симуляции физико-химических процессов. Для обучения ИИ «заточена» модель ПИ XE9680. Младшая модель ПИ 760XA может использоваться как для обучения, так и для инференса (работы уже обученной модели).

Рис. 3. ▶
Crusader HPC Squire 4245R

Рис. 4. ▶▶
Сервер ДатаРу ПИ XE9680

В основе модели ПИ XE9680 – восемь модулей GPU Nvidia H100 SXM и процессоры Intel 4-го поколения с оперативной памятью до 2 Тбайт.

Планы развития DataPy включают расширение линейки ИИ-серверов и возможных конфигураций, а также использование новейших GPU. Например, компания уже готова поставлять оборудование с GPU-модулями Nvidia H200, которые были презентованы компанией Nvidia в ноябре 2023 г. Кроме того, DataPy собирается в сотрудничестве с ведущими российскими разработчиками систем на базе ИИ расширить список программно-аппаратных комплексов.

Delta Computers

В конце 2023 г. компания представила Delta Sprut, платформу GPGPU (General Purpose GPU), целевое назначение которой, по заявлению компании, – системы искусственного интеллекта, в том числе платформы OpenAI/ChatGPT, машинное обучение, нейронные сети, машинное зрение и перевод, высокопроизводительные вычисления, 3D VDI в задачах проектирования и работе со сложными 3D-моделями.

Платформа Delta Sprut позволяет существенно увеличить возможности подключения PCIe-устройств к серверу: модуль имеет четыре разъема с интерфейсом PCIe x16 и допускает установку четырех карт HHHL или двух карт FHFL. В режиме каскадирования к одному серверу можно подключить до восьми GPU двойной высоты или до 16 GPU стандартной высоты. В Delta Sprut используются GPU Nvidia A100, Nvidia H100 и AMD Instinct, но можно устанавливать графические ускорители и других производителей. Для устройств Nvidia поддерживается попарное объединение мостами NVLink последнего поколения.

В 2016 г. Delta Computers стала первым российским участником проекта Open Computer Project (OCP), поэтому неудивительно, что платформа Delta Sprut соответствует стандартам OCP. Как отмечают в компании, у клиентов, которые уже используют в своей инфраструктуре оборудование стандарта OCP, не возникнет проблем при установке нового продукта. При этом серверное шасси Delta Sprut можно интегрировать в 19-дюймовое оборудование.

В Delta Computers указывают, что решение компании позволяет сократить затраты на инфраструктуру и энергопотребление. По их словам, объем графической памяти, предоставляемый 40 OCP-серверами с двумя GPGPU-платформами Delta Sprut, эквивалентен объему, который другие производители могут реализовать только на 80 стандартных 19-дюймовых серверах.

Платформа Delta Sprut, как и другие продукты Delta Computers, включена в Единый реестр российской радиоэлектронной продукции (ЕРРРП), который ведет Минпромторг.

GAGAR>N

В ответ на рост спроса на серверное оборудование для реализации проектов, связанных с искусственным интеллектом, компания GAGAR>N не только усовершенствовала существующие модели серверов, но и разработала новые специализированные продукты. Решения компании ориентированы как на обучение моделей на основе больших объемов данных (для этого предлагаются модульные масштабируемые системы с большой вычислительной мощностью процессоров GPU), так и на инференс (для этого подойдут модульные серверы с установленными компактными адаптерами).

Основной продукт GAGAR>N для ИИ-задач – это модуль JBOG, занимающий 2U и позволяющий разместить до восьми полноразмерных двухслотовых адаптеров GPU или до 16 однослотовых. Модуль может быть подключен к одному серверу для повышения его производительности либо к нескольким серверам (до четырех) с обеспечением необходимой изоляции.

Для задач инференса пригоден сервер Оракул Gen2 на базе Intel Xeon Scalable 3-го поколения с установленными адаптерами GPU. Сервер имеет до 80 ядер на сервер, 32 слота оперативной памяти DDR4, восемь дисков NVMe/SSD с возможностью «горячей» замены, четыре накопителя NVMe и два накопителя M.2. Продукт включен в ЕРРРП.

GAGAR>N использует центральные процессоры Intel и GPU-модули от Nvidia. Коммуникационная среда в большинстве проектов реализуется на основе стандарта 100G Ethernet. Для хранения данных рассматриваются программно определя-

◀◀ Рис. 5. GPGPU-платформа Delta Sprut

◀ Рис. 6. Сервер GAGAR>N Оракул Gen2

емые решения, причем аппаратной платформой хранения служат серверы с масштабируемой дисковой подсистемой.

Все продукты GAGAR>N отвечают принципам и подходам OCP. При планировании продуктового портфеля компания ориентируется как на мировые технологические тенденции, так и на реальный спрос со стороны российских заказчиков. В перспективе – новые поколения устройств, а также расширение линейки за счет установки процессоров GPU разных форм-факторов и специализированных плат отечественных производителей.

iRU

Для приложений ИИ компания iRU разработала и выпускает сервер Rock G2212IG4. Компоновка сервера позволяет установить до двух полноразмерных GPU-ускорителей, а также два процессора на базе Intel Xeon Scalable 4-го или 5-го поколения и до 8 Тбайт памяти DDR5 ECC REG. В качестве графических ускорителей могут использоваться GPU Nvidia A100 и др. Предусмотрены варианты с 16 накопителями 3,5/2,5" HS (SATA/SAS/NVME), M.2 (Type 2280/22110) SATA и 2,5" HS SATA Rear, что обеспечивает большую пропускную способность и лучшую целостность данных. Сервер имеет слоты расширения, соответствующие стандарту OCP 3.0.

Как отмечают в компании, широкий выбор конфигураций сервера iRU Rock G2212IG4 предоставляет пользователям возможность решать сложные задачи в различных сферах: торговле, медицине, промышленности, логистике, банковском секторе и научных исследованиях. iRU имеет разветвленную сеть сервисной поддержки, насчитывающую, по данным компании, 180 собственных сервисных центров по всей стране.

В ближайших планах iRU – выпуск модели с поддержкой до 10 графических ускорителей.

OpenYard

Для приложений, требующих графических ускорителей, в том числе для задач в области ИИ, машинного обучения и нейросетей, компания OpenYard предлагает сервер RS201. Это GPU-ready решение, в которое может быть установлено до трех графических адаптеров. Модель RS201 поддерживает до 128 ядер (256 потоков), до 8 Тбайт оперативной памяти DDR4, до 780 Тбайт памяти на накопителях NVMe SSD и до восьми плат расширения PCIe в зависимости от реализации. Разъемы PCIe соответствуют спецификациям OCP 2.0 и OCP 3.0. Сервер оснащен двумя резервными блоками питания мощностью до 2400 Вт, что должно обеспечивать надежную и бесперебойную работу. Продукт включен в ЕРРРП.

Как сообщили представители OpenYard, компания контролирует качество своей продукции с помощью шестиэтапной системы проверки, охватывающей все стадии производства. Для подтверждения надежности серверы после сборки проходят стресс-тестирование в течение 6–8 ч.

Компания планирует расширять существующую линейку, а также разрабатывать как более «легкие» серверы, так и специализированные решения. Вместе со стратегическим заказчиком OpenYard работает над несколькими концептами серверов для видеоускорителей. В компании отметили, что готовы к стратегическим альянсам, в том числе в контексте ИИ-разработок.

«Гравитон»

Компания выпускает несколько моделей серверов, ориентированных на поддержку ИИ-приложений. Как считают в «Гравитон», для задач ИИ подходят серверы на базе процессоров Intel Xeon Scalable 4-го и 5-го поколений, построенные на новой материнской плате «Урал» и имеющие до 8 Тбайт оперативной памяти, а также оснащенные большим количеством накопителей (HDD и SSD). Для высокопроизводительных вычислений компания предлагает линейку серверов C2000A с процессорами AMD EPYC. Эти решения построены на материнской плате «Арктика» и могут иметь до 4 Тбайт оперативной памяти. По словам А. Фильченкова, стоимость одного ядра в таком решении почти в два раза ниже, чем у аналогичных продуктов.

Для задач, связанных с генерацией визуального контента на основе технологий ИИ, «Гравитон» предлагает GPU-серверы C2084И форм-фактора Tower/4U на материнской плате «Тундра». Эти серверы могут нести «на борту» до пяти графических ускорителей Nvidia Quadro RTX A5000/A6000 и линейки Nvidia V100/A40/A100.

Рис. 7. ▶
Сервер iRU Rock G2212IG4

Рис. 8. ▶▶
Сервер OpenYard RS201

В плане развития линейки ИИ-серверов компания ориентируется на последние достижения в ИТ-индустрии. В частности, «Гравитон» планирует использовать в своих новых серверах процессоры Intel Xeon 6-го поколения и AMD EPYC 5-го поколения по мере их появления на рынке.

Серверы для ИИ-приложений в числе других решений «Гравитон» включены в ЕРРРП и Реестр российской промышленной продукции Минпромторга.

«Тринити»

Для приложений на основе ИИ-технологий, таких как обучение нейронных сетей, обработка и анализ больших данных для выявления закономерностей, видеоаналитика, обработка речи в задачах, связанных с пониманием и генерацией текста, и рекомендательные системы, «Тринити» предлагает универсальные платформы, которые могут быть оптимизированы для работы с высокими вычислительными нагрузками. В серверы могут устанавливаться как модули GPU, так и TPU или FPGA.

Компания комплектует свои серверы процессорами Intel Xeon Scalable 4-го и 5-го поколений и AMD EPYC; GPU Nvidia Tesla (серии V100, A100, H100) и AMD Radeon Instinct, а также накопителями NVMe SSD, NAS и SAN для масштабируемого хранения данных.

Почти два десятка моделей серверов «Тринити» включены в ЕРРРП. Компания планирует интегрировать свои решения с облачными платформами.

Сколько ватт на стойку

Для цодостроителей одним из важных следствий бума ИИ может стать существенное повышение мощности серверов, обеспечивающих работу ИИ-приложений. Не исключено, что это потребует пересмотра архитектуры системы охлаждения – одного из ключевых компонентов инженерной инфраструктуры ЦОДов. Идут разговоры даже о массовом переходе на прямое жидкостное охлаждение, которое сейчас не используется в большинстве дата-центров, полагающихся на воздушное охлаждение. Какова может быть мощность серверной стойки, заполненной ИИ-серверами?

Энергопотребление и соответственно тепловыделение серверов во многом определяется конфигурацией и нагрузкой. Например, по данным «Тринити», 1U-серверы обычно потребляют 300–800 Вт, но в зависимости от количества и типа установленных компонентов, таких как высокопроизводительные GPU, потребление может доходить до 800–2000 Вт на сервер.

Как сообщили в компании GAGAR>N, энергопотребление одного модуля JBOG (2U) с восемью адаптерами может превышать 3 кВт, а энергопотребление одного шкафа – доходить до 18 кВт и выше. А по данным iRU, в максимальной конфигурации тепловыделение сервера в пересчете на 1U достигает 1 кВт.

Получается, что даже если типовую стойку «набить» ИИ-серверами, то общая мощность составит примерно 40 кВт. (Правда, эта «набивка» необязательно окажется оптимальной с точки зрения экономики проекта.) Но и такое тепловыделение вполне можно снять воздушным охлаждением. Поэтому традиционное охлаждение еще рано списывать со счетов, а массовый переход на прямое жидкостное охлаждение ожидает нас не «прямо сейчас».

От архитектуры до сервиса

Как мы видим, большинство производителей ИИ-серверов используют связку CPU Intel или AMD и GPU Nvidia. Вероятно, сегодня этот подход оптимален по соотношению «цена – качество». Типовой состав таких решений следующий:

- высокопроизводительные CPU (Intel или AMD) с несколькими ядрами и поддержкой многопоточности;
- мощные GPU с большим количеством ядер и высокой производительностью для параллельных вычислений (обычно Nvidia A100, H100);
- объем оперативной памяти, достаточный для обработки больших объемов данных и хранения промежуточных результатов;
- быстрое хранилище данных (NVMe SSD) для минимизации времени доступа к данным;
- высокоскоростные сетевые интерфейсы (100GbE) для быстрой передачи данных между серверами и хранилищами.

Несмотря на понятную ориентацию производителей серверов на GPU Nvidia, полезна возможность использовать в серверах графические ускорители разных вендоров. В условиях санкционного давления такая универсальность даст большую уверенность в дальнейшем развитии инфраструктуры с применением GPU.

Кроме того, при работе со столь сложными решениями, как серверы для ИИ, критически важна техническая поддержка. Поэтому заказчикам следует обратить внимание на наличие разветвленной сети сервисных центров, что позволит быстрее решать вопросы, связанные с работоспособностью серверов.

Как вы могли заметить, в этом обзоре представлены далеко не все отечественные производители серверов. В частности, Nerpa, Sitronics и «Аквариус» на момент его подготовки не предлагали специализированных серверов для ИИ. Но почти не сомневаемся в том, что и эти производители в ближайшее время такие решения предложат. ИКС

Возможность использовать в серверах графические ускорители разных вендоров даст большую уверенность в дальнейшем развитии инфраструктуры с применением GPU

Итальянские системы охлаждения в России: профессионализм и стабильность

Европейское качество, точность исполнения и проверенные технологии – принципы, которые компания HiRef сохраняет на российском рынке, несмотря на изменившиеся условия. Василий Новиков, директор по развитию HiRef Rus, рассказывает, как компания адаптируется к новым реалиям и какие решения предлагает заказчикам.

– HiRef – хорошо известный российским специалистам производитель систем охлаждения для ЦОДов. Что изменилось в работе компании за последние 2,5 года?

– С февраля 2022 г. нам уже миллион раз задавали и задают одни и те же вопросы: возите ли оборудование, как возите, официальные ли это поставки? На самом деле за последние 2,5 года для нас ничего не поменялось. Но чтобы прояснить для всех ситуацию, повторю: мы официальное представительство итальянского завода HiRef в России, мы осуществляем официальные прямые поставки оборудования с завода в Италии, получая в органах ЕС все необходимые разрешения на вывоз. Мы в полном объеме осуществляем техническую, сервисную, гарантийную и постгарантийную поддержку оборудования HiRef в РФ.

Да, за последние 2,5 года рынок кардинально изменился. Но, несмотря на все пертурбации, активизацию российских производителей, китайских коллег и ценовые войны, наши продажи только выросли.

– Однако у заказчиков есть неуверенность в отношении поставок из Европы. Как ее убрать?

– А у меня встречный вопрос: когда заказчик рассматривает китайские бренды, где гарантия, что их оборудование приедет? То юань «не ходит», то обострения на Тайване, то неожиданно возникают логистические трудности. В текущей геополитической ситуации полностью исключить риск, связанный со страной изготовления, нельзя. Если раньше рынок жил планами на три-пять лет, то сегодня часто приходится планировать в горизонте трех месяцев.

– Но сроки поставки «тяжелого» чиллера отнюдь не три месяца. Какова ситуация с логистикой?

– Сроки производства действительно могут варьироваться, но в нашем случае они близки к доковидным. Специфика состоит в том, что российские клиенты заказывают много нестандартного оборудования. Любой крупный клиент с ЦОДом мощностью 1–2 МВт и выше всегда хочет чего-то индивидуального: особые требования к вводам, режимам работы, протоколам диспетчеризации. Выполнение этих требований увеличивает сроки поставки. Приведу пример, когда мы вместе с заводом изготавливали оборудование для конкретного заказчика. С момента формулирования ТЗ на все ушло девять месяцев. Три месяца занимались перерасчетами. Потом сделали опытный образец. Заказчик поехал его смотреть и, как водится, внес еще корректировки. После чего мы изготовили продукт с учетом всех пожеланий заказчика. Это творческий процесс. И этим, кстати, мы, европейские производители, отличаемся от азиатских коллег, которые больше ориентированы на повторение, копирование одного и того же оборудования.

– Но так дешевле…

– Конечно, копирование оборудования, максимальная унификация моделей, компонентной базы – все это снижает себестоимость продукта. Европейская школа немного другая. Европейские производители делают ставку на энергоэффективность и технологичность. По сути, каждая более или менее мощная машина индивидуальна. Это позволяет добиться высокой производительности и соответствия специфическим требованиям.

– Но ведь и у вас есть типовые решения?

– Есть, например, для небольших серверных до 100 кВт. Им не нужны специальные решения, достаточно обычных прецизионных кондиционеров. Такие решения у нас есть на складе в Москве. Там около 50 единиц оборудования, фреоновые кондиционеры 10–50 кВт, унифицированные, в типовой комплектации, с увлажнителем, EC-вентиляторами, картой диспетчеризации по SNMP.

– Мы перешли к рассмотрению оборудования. Какие вообще решения HiRef предлагает для ЦОДов?

– В нашем портфеле есть любые решения, фреоновые и с водяным охлаждением. Есть чиллеры и холодные стены. Есть системы фрикулинга с воздушным рекуператором. Есть адиабатика. Есть системы прямого жидкостного охлаждения серверов. Есть верхнеуровневая система управления. Есть комплексное решение со стойками, изоляцией коридора и пр. Сегодня это решение востребовано все больше.

– Что из этого наиболее востребовано в России?

– В первую очередь «классика»: внутрирядные и шкафные кондиционеры на фреоне, на воде и, конечно, чиллеры.

В последнее время много запросов на холодные стены. Однако хочу предостеречь заказчиков. На первый взгляд, холодная стена – вещь несложная: корпус, теплообменник,

энное число вентиляторов. Но есть еще одно важное звено: контроллер и его ПО. Европейские компании оттачивали это ПО лет 20–30, а то и больше. Ряд же новых производителей пытаются сделать его по-быстрому, «на коленке». Я был бы крайне осторожен в использовании подобных изделий.

– За последний год заметно вырос интерес заказчиков к решениям на основе фрикулинга. Что скажете про этот тренд?

– Этот тренд в той или иной степени был всегда, потому что фрикулинг позволяет экономить. Все, кто связан с крупными ЦОДами, с высоким энергопотреблением, все хотят экономить.

Фрикулинг обычно делается на базе приточно-вытяжных установок (ПВУ). Вещь это неновая, она появилась намного раньше прецизионных кондиционеров. Более того, ряд российских предприятий давно выпускает подобные установки. Но обычная ПВУ никак не дотягивает до того уровня, который требуется в ЦОДе. Дело, как и в случае с холодными стенами, в ПО автоматизации, которое европейские компании разрабатывают и совершенствуют десятки лет. Если не рассматривать ПВУ как воздуходувку для офиса, если речь идет о ЦОДе, где нужен расчет воздушного баланса, температурных колебаний и т.д., вам потребуется продвинутая система автоматизации. В России таких систем нет. И в Китае нет.

Короче говоря, фрикулинг – это не так легко и просто, как многие считают. У нас такие решения есть. С готовыми «мозгами». Есть и инсталляции в России, например, в ЦОДах одного из операторов большой тройки.

– Непосредственно с фрикулингом связана адиабатика, которая часто используется для доохлаждения в системах фрикулинга. Как оцениваете перспективы этой технологии?

– Технология модная. Но хотел бы обратить внимание на два момента. Первый – резервирование, необходимое для соответствия требованиям Tier III и Tier IV. Адиабатика – это очень большой расход воды. Надо иметь несколько источников, огромный резервуар с водой.

Второй момент связан с тем, что российские заказчики, решившись на установку системы фрикулинга с адиабатикой, начинают сомневаться: «а если не вытянет», «а если будет жаркий год»... И в результате для резервирования ставят в параллель фреоновую или чиллерную систему. Две системы – дорого и громоздко.

В Европе немного другие температурные режимы. Там климат мягче. Да и само построение ЦОДа больше ориентировано не на отказоустойчивость, а на экономию электроэнергии, на «зеленую» энергетику. Кроме того, в Европе готовы в два-три раза увеличить CAPEX, чтобы потом экономить на OPEX. А у нас хотят сэкономить и там и там. Так не получается.

– Интерес к искусственному интеллекту вызвал разговоры о резком повышении мощности ИТ-стоек. Говорят про 50 и даже 100 кВт на стойку. Что думаете о перспективах прямого жидкостного охлаждения?

– Знаю ряд небольших объектов, где установлены, скажем, пять кондиционеров, из них работает один, и чтобы он работал, помимо ИТ-стоек стоят еще две тепловые пушки. И заказчики недовольны. Причина этого в следующем: заказчик решил, что у него будет, например, 20 кВт на стойку. Проектировщик переразмерил на 30% (стандартная практика всех проектировщиков еще со времен СССР), потом генподрядчик – еще на 30%. В итоге всех фантазий производительность инженерных систем в несколько раз превышает реальные потребности. Да еще и стойку сразу заполнить ИТ-оборудованием не получается...

Надо быть реалистом в отношении нагрузок. Я не говорю про суперкомпьютеры, где все должно быть компактно. Если есть возможность избежать высокой плотности мощности, лучше распределять нагрузку так, чтобы тепло можно было снимать классическими проверенными способами.

У HiRef есть решения для прямого жидкостного охлаждения серверов, но в целом на рынке пока реализовано не так много подобных проектов. Реальные тепловые нагрузки зачастую ниже заявленных, и системы охлаждения оказываются избыточно мощными, что приводит к неэффективному использованию ресурсов.

– Что в ближайших планах HiRef?

– Если говорить о заводе HiRef в Италии, то в ближайшие месяцы планируется завершение строительства и ввод в эксплуатацию второй очереди завода. Производительность завода вырастет в два раза, что существенно ускорит и выполнение заказов из России.

Если говорить о HiRef Rus, то сегодня у нас в приоритете развитие сервиса, наращивание соответствующих компетенций. Оборудование дорогое, требует особого, профессионального внимания. Не просто прийти посмотреть, галочку поставить, а проверить, настроить, поднастроить, адаптировать, перенастроить, провести упредительный ремонт и т.д. Это особенно важно, когда речь идет о критической инфраструктуре. Кроме сервиса мы усилили направления пусконаладки и эксплуатации. Для крупных заказчиков проводим обучение службы эксплуатации прямо на объекте.

– Для критической инфраструктуры ЦОДов важна оперативность устранения неполадок в случае инцидента или аварии. Что вы рекомендуете?

– Первое: не паниковать. Знаю примеры, когда все зарезервировано по схеме 2N, что-то сгорело или подгорело и начинается паника. Спокойно, есть резервное оборудование. Если оно грамотно обслуживалось, все будет хорошо. Можно, конечно, помимо резерва нанять компанию, которая будет в любое время суток в течение 15 мин приезжать на объект и все ремонтировать. Но такое сопровождение стоит больших денег.

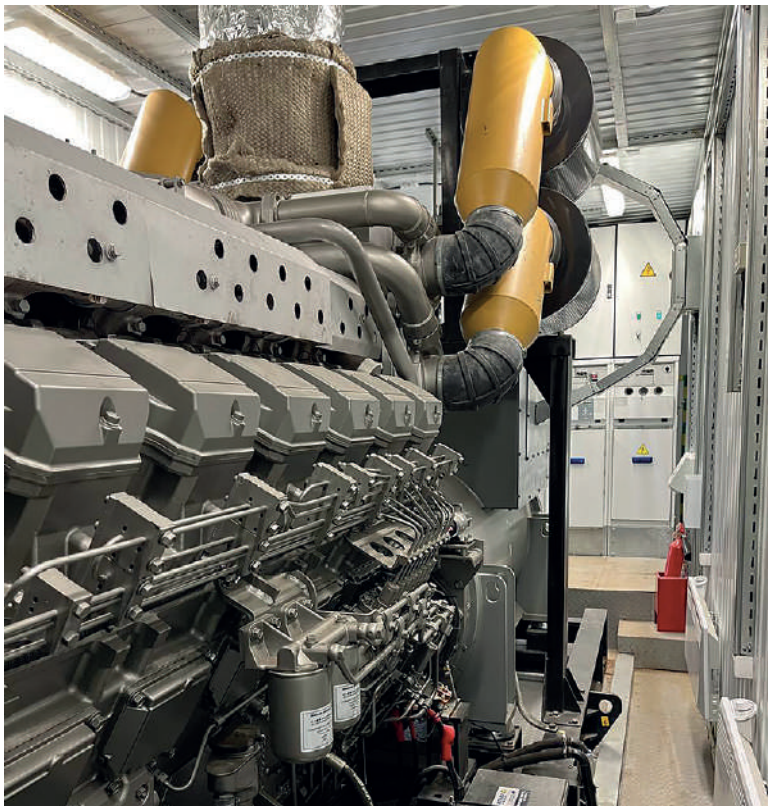
Второй момент. В текущей ситуации я бы рекомендовал держать на объекте определенный ЗИП. Раньше большую часть комплектующих, включая компрессоры и вентиляторы, можно было оперативно купить в России со складов официальных поставщиков. Сейчас ситуация поменялась: все это можно достать, например, через нас, через завод, но сроки другие. Хотя некий ЗИП мы держим у себя на складе, на объекте он необходим тоже.

Мы уверены, что грамотный вдумчивый подбор оборудования, профессиональный сервис и обученная служба эксплуатации – залог надежной и эффективной работы любого дата-центра.

ДГУ в России: поиски пути

Екатерина Шлык

Уход зарубежных вендоров, увеличение числа дата-центров, рост угроз в сфере энергетической безопасности, борьба за энергоэффективность и новые подходы к обеспечению отказоустойчивости – вот лишь некоторые из факторов, влияющих на состояние и развитие современного российского рынка ДГУ.



Ситуацию на российском рынке дизель-генераторных установок (ДГУ) для дата-центров обсуждали участники дискуссии «Современные тенденции применения ДГУ в ЦОДах», состоявшейся в рамках организованного «ИКС-Медиа» 19-го форума «ЦОД». Эмоциональность и интенсивность дискуссии, а также полярность мнений участников свидетельствуют, что однозначного видения ситуации нет, но поднятые вопросы чувствительны и актуальны.

Двигатели для российских ДГУ: борьба между Западом и Востоком

«Сердце» дизель-генераторной установки – двигатель. Конкурентная среда на рынке двигателей для ДГУ такова: отечественные производители решений для дата-центров не предлагают, поэтому до недавнего времени большинство ДГУ были построены на базе продуктов западных вендоров, в первую очередь Cummins, Caterpillar, MTU. Однако в последние годы на российский рынок активно выходят производители из КНР и, по прогнозам игроков отрасли, в ближайшем будущем именно китайская продукция будет доминировать на рынке.

Каждый из вариантов имеет свои плюсы и минусы. Достоинства западных продуктов – известный уровень качества, предсказуемость, большой опыт эксплуатации. Недостатки очевидны и являются следствием введенных санкций и массового ухода вендоров с рынка. Правда, часть этих проблем решается благодаря программам параллельного импорта, но все же потенциальных и реальных проблем стало намного больше.

Что касается продукции китайских вендоров, то их безусловные достоинства – широкий выбор, относительно быстрая доставка, заинтересованность вендоров в сотрудничестве и, конечно, цены, особенно в сравнении с западными продуктами. А главная из проблем – непредсказуемость уровня качества. Наряду с решениями, действительно не уступающими западным образцам, встречаются и такие, которые не выдерживают никакой критики. Это обстоятельство в сочетании с недостатком объективной информации (а порой – и документации) от поставщиков превращает использование китайских решений в своего рода рулетку. Но со временем появится необходимый опыт взаимодействия. Причем, по общему мнению участников дискуссии, ключевую роль в накоплении опыта работы с китайскими поставщиками будут играть не конечные потребители, а отечественные поставщики, интеграторы и компании, занимающиеся пакетированием ДГУ. Именно они, взаимодействуя с различными поставщиками и их решениями, постепенно сформируют четкое представление о продукции и возможностях тех или иных вендоров.

Здесь стоит сказать о крайне интересной инициативе, которую в настоящее время реализует компания «Ючай» (Yuchai). Как сообщил Владимир Кириченко, коммерческий директор компании «Альфа Балт Инжиниринг», партнера вендора, достигнуто официальное соглашение о локализации производства двигателей для ДГУ в России. На первом этапе это будет сборка гото-

вых узлов, но постепенно российская сторона будет брать на себя все больше работ, и на финальном этапе (ориентировочно – лет через пять) в России будет выполняться весь цикл производства, включая литье.

Возможно, благодаря локализации на рынке появится явный лидер, который будет предлагать не только техническое решение, но и гарантии, сервисное обслуживание и возможность быстрого ремонта. Упростится в этом случае и деятельность тех компаний, которые занимаются пакетированием ДГУ, потому что будет легче и быстрее обеспечивать совместимость решений.

Все дело в проектировании

Надежность ДГУ определяется не только и, по мнению некоторых экспертов, не столько страной производства двигателя, сколько тем, как собрана сама установка. То есть пакетированием, которое выполняется в России.

Например, по опыту технического директора IXcellerate Сергея Вышемирского, чаще всего проблемы дизель-генераторных установок связаны не с дизелем, а с теми их частями, за которые отвечают проектировщики ДГУ. Проблемы эти могут быть разнообразными, от конструктивных (нерациональное расположение элементов) до некорректной работы контроллеров или нефункционирующей автоматики. Поэтому, полагает эксперт, обсуждать надо не производителей дизелей, а проектировщиков готовых установок – именно от них в наибольшей степени зависит работоспособность и надежность всего модуля.

При этом на деле альтернативы отечественным пакетировщикам нет. Купить весь модуль ДГУ в сборе за рубежом – вариант нерабочий. Слишком велики в разных странах различия в нормативных требованиях, в условиях эксплуатации. Кроме того, сложности согласования при таком подходе близки к непреодолимым.

Суммируя вышесказанное, констатируем: рынку остро необходимы отечественные компании-проектировщики, которые обладают одновременно глубокой экспертизой и ответственными и опытными инженерными кадрами и внимательно относятся к нуждам заказчиков. Иными словами, рынку остро необходим сервис.

Обслуживание ДГУ: свои и чужие

Проблемы сервисного обслуживания в области ИТ – это та тема, которая, пожалуй, наиболее часто всплывает в разговорах специалистов после ухода с российского рынка западных вендоров. И область ДГУ – не исключение. Причем речь идет не о собственно обслуживании ДГУ, уточняет директор по развитию компании «Хайтед» Михаил Саликов. Дизель одного производителя не настолько отличается от продукта другого вендора, чтобы инженерам потребовались какие-то принципиально новые знания или умения. Речь идет в первую очередь о том, как складываются отношения поставщика и заказчика, какие обязательства и гарантии дают одни и ждут другие. И это уже совсем иная история, пока рынком не вполне отработанная.

Например, «Хайтед» как поставщик инженерных решений перешел на проактивный сервис обслуживания ДГУ, не просто предлагая заказчикам плановое ТО устройства, но беря на себя обязательства по его техподдержке и обеспечению работоспособности. Вплоть до того, что на одном из объектов заказчика на постоянной основе работает инженер «Хайтед», в обязанности которого входит постоянный контроль за работой ДГУ. Однако в условиях дефицита квалифицированных кадров сделать такой подход повсеместным вряд ли получится, добавляет М. Саликов.

Если владельцам небольших объектов подобный on-site сервис может быть интересен, то применительно к крупным дата-центрам его ценность сомнительна, указывает С. Вышемирский. В больших ЦОДах, где установлены десятки ДГУ, нужен не один специалист, а целая команда высококвалифицированных и – главное –

Источник: «Хайтед»

ДГУ Cummins

ДГУ Yuchai мощностью 1000 кВт

Источник: «Альфа Балт Инжиниринг»

Источник: IXcellerate

ДГУ, установленные в ЦОДе IXcellerate

заинтересованных специалистов. Для стороннего инженера ДГУ в ЦОДе заказчика – чужой объект, таким людям можно доверить «разве что замену масла», подчеркивает технический директор IXcellerate. У компании были прецеденты, когда ДГУ выходила из строя сразу после проведенной сторонней компанией проверки или когда проверяющие не замечали явных неисправностей. Так что единственным приемлемым вариантом сервисного обслуживания ДГУ в крупных дата-центрах эксперт считает формирование собственной команды специалистов.

Синкретическую модель предпочитают в Сбере. По словам Сергея Лебедева, заместителя начальника управления сопровождения ЦОД компании, Сбер вполне устраивает тот уровень услуг, которые оказывает подрядчик. Однако для предотвращения неожиданностей деятельность подрядчика всегда контролируется внутренними специалистами.

Есть ли альтернативы ДГУ?

Говоря о «темной стороне» ДГУ в ЦОДах, обычно упоминают, что на ДГУ приходится до 15% CAPEX при строительстве ЦОДа, но значительную часть времени установки простаивают и лишь потребляют ресурсы, требуя регулярного обслуживания и контроля. Кроме того, ДГУ «съедают» довольно большую площадь сами по себе, а также зачастую требуют организации дополнительного топливохранилища и специальных коммуникаций для отведения отходов. Наконец, подавляющее большинство ДГУ работает на невозобновляемых источниках энергии (продуктах нефтепереработки), что мешает достижению целей устойчивого развития. Естественно, у операторов дата-центров велико искушение минимизировать издержки и более целевым образом использовать площадь. Так что разговоры о том, что отрасль ЦОДов движется к сокращению использования ДГУ, ведутся не один год. Но говорить о массовом отказе операторов дата-центров от ДГУ пока очень и очень рано. Наоборот, по словам Антона Гущина, руководителя проектов компании ПСМ, количество запросов на решения с ДГУ растет, в том числе на мощные установки.

Здесь нужно отметить, что на данный момент есть два основных способа, с помощью которых оператор ЦОДа может уменьшить количество ДГУ, – это использование возобновляемой энергии и ИТ-решения (резервирование работы ИТ-нагрузки на уровне сети дата-центров). Но если принять во внимание, что развитие и надежность источников возобновляемой энергии в России находятся на недостаточном уровне и, как ранее писал С. Вышемирский, полагаться на них в критических ситуациях нельзя, то реальные альтернативы ДГУ сокращаются до одной – резервирования ИТ-ресурсов.

Так, по словам С. Лебедева, Сбер ведет работу в направлении того, чтобы обеспечивать резервирование на уровне ИТ-систем (как, например, частично делает «Яндекс», что позволило ему уменьшить количество используемых ДГУ). Но на данный момент компания не рассматривает отказ от ДГУ или даже сокращение числа установок – несмотря на то, что, скажем, в мегаЦОДе Сбербанка «Южный порт» ДГУ за более чем 10 лет работы не понадобились ни разу. «Если резервирование не поддерживается ИТ-ресурсами, уменьшать использование ДГУ можно только в том случае, если компании неважно, “лег” у нее ЦОД или нет», – уверен С. Лебедев.

Еще более категоричен С. Вышемирский. Зимой 2024 г., в сильные холода, когда происходили веерные отключения электричества, так как энергосети не справлялись с нагрузкой, ЦОДам IXcellerate пришлось некоторое время работать на ДГУ, и только это позволило компании выполнить все обязательства перед клиентами в критической ситуации. Поэтому он выступает однозначно за использование установок, полагая что реальной альтернативы им нет. Впрочем, чтобы обезопасить дата-центр в экстренной ситуации, говорит С. Вышемирский, нужны не только ДГУ. Необходимы новые правила подключения дата-центров к питающим центрам. Речь идет о том, что линия второй категории энергоснабжения должна быть действительно резервирующей, а не прокладываться в параллель с первой по одной траншее от одного питающего центра. Две линии, два разнесенных центра – правило должно быть именно таким.

Поддерживает мысль о том, что отказ от ДГУ несет в себе слишком большие риски, и М. Саликов. По его словам, ДГУ в ЦОДе можно сравнить с подушкой безопасности в автомобиле: очень хорошо, если за все время эксплуатации она не пригодилась, но в ситуации, когда она окажется нужна, это спасет жизнь. ИКС

От аккумуляторов до стоек и PDU мирового уровня

Компания ENERGON анонсировала выпуск стоек и блоков распределения питания для ЦОДов. О новинках рассказывает директор департамента развития новых продуктов Александр Беспалов.

– Почему компания решила расширить ассортимент продукции и обратиться к выпуску PDU?

– Компания ENERGON – лидер российского рынка аккумуляторных батарей и литий-ионных накопителей, в том числе для дата-центров. Мы четверть века работаем с заказчиками и хорошо понимаем их проблемы. Два года рынок пытается адаптироваться к уходу глобальных брендов, поставлявших качественное оборудование, но дефицит сохраняется, в том числе в области стоек и блоков распределения питания (PDU).

Раньше для российских производителей нормой были PDU без контроллеров, обеспечивающих мониторинг и управление розетками. Теперь многие предлагают Smart PDU, но по функциональности они уступают продуктам глобальных брендов. Мы решили исправить ситуацию и выпустить линейку PDU под брендом SMARTWATT, которые ни в чем не уступают аналогичным решениям мировых лидеров.

– В чем особенности конструктива PDU SMARTWATT и сетевого контроллера? В чем конкурентные преимущества новой линейки продукции?

– В продукции SMARTWATT используется уникальный механизм фиксации разъема кабеля в розетке, который предотвращает случайное выпадание или вынимание кабеля. Он удобнее и надежнее, чем у конкурентов. При этом силовые розетки могут быть универсальными, поддерживать кабели с разъемами C13 и C19 одновременно, с функцией фиксации, без дополнительных адаптеров. Это дает возможность не менять PDU, если требуется подключить оборудование с другим разъемом.

В PDU используются гидромагнитные выключатели с защитой от случайного отключения, позволяющие эксплуатировать PDU при температурах до 60°C. В составе линейки есть и бюджетные модели с электромеханическими автоматическими выключателями и алюминиевым шасси, но даже они отличаются от решений конкурентов более высоким качеством.

Другое достоинство PDU SMARTWATT – компактность и плоский дизайн. Сечение корпуса квадратное, без утолщения, часто мешающего при эксплуатации стоечного оборудования. Решения кастомизированные – можно заказать любую цветовую гамму корпуса и розеток, разные типы и число разъемов, сгруппировать однофазные и трехфазные розетки, установить индивидуальные типы управления и защиты.

Все модели линейки, кроме базовой (PDU B), поддерживают каскадное подключение – соединение до 32 устройств и передачу данных. Такой каскад подключается к одному контроллеру, обеспечивая экономию на дополнительных модулях сбора сигналов. Контроллер PDU имеет функцию «горячей» замены, что важно для непрерывно работающих дата-центров. Кроме того, он поддерживает все современные протоколы, включая SNMP v3, HTTPS, IPv4 и IPv6, для интеграции решения с системами DCIM или SCADA.

– Почему компания решила заняться еще и серверными шкафами?

– Шкафы для размещения нашей основной продукции – свинцовых и литиевых батарей – мы предлагаем давно. Теперь решили заняться серверными шкафами, поскольку сейчас качественных решений на российском рынке не хватает. Несмотря на то что многие серверные шкафы производятся в России, срок их изготовления и поставки может достигать нескольких месяцев, да и стоимость неоправданно высока.

Мы предлагаем две серии шкафов SMARTWATT RACK: «Премиум» (P-Series) и «Стандарт» (S-Series). Шкафы выдерживают статическую нагрузку до 1800 кг и со временем не начинают расшатываться. У большинства конкурентов толщина металла 1–1,5 мм, в наших шкафах – 1,5–2 мм. При изготовлении рамы используется технология холодного проката профилей, значительно увеличивающая жесткость металла. Все это повышает надежность конструкции шкафа.

В ЦОДах иногда возникает необходимость перемещения нагруженной стойки, при котором возможна ее деформация. Наши шкафы «Стандарт» выдерживают динамическую нагрузку до 1000 кг, а «Премиум» – до 1200 кг. При этом на российском рынке считаются хорошими шкафы, выдерживающие динамическую нагрузку 500–800 кг.

На охлаждение серверов влияет перфорация дверей. В серии «Стандарт» она более 76%, в «Премиум» – более 80%, причем процент подсчитывается от полной площади двери, а не от перфорированной зоны, как у некоторых производителей.

Много внимания уделено полезным мелочам. Внутренние профили и направляющие оцинкованы и покрашены, есть маркировка направляющих, чтобы видеть, на какой высоте размещается оборудование. Заземление двери выполнено быстросъемным кабелем, который, как и дверь, снимается без инструментов. Сама сборка шкафа удобная и простая, занимает в среднем от 15 мин.

– Когда новая продукция будет доступна на рынке?

– PDU и серверные шкафы SMARTWATT будут доступны к покупке с ноября 2024 г.

Чем тушить ЦОДы

Кевин Хэслер, директор специальных проектов, Uptime Institute

В Uptime Institute полагают, что для большинства ЦОДов лучше всего подходят системы пожаротушения на основе воды с сухими трубами и клапанами предварительного действия. Системы с инертными газами при срабатывании могут повредить ИТ-оборудование, а галогенуглеводородные очень дороги.

Пожар на любом объекте – явление страшное, и ЦОДы здесь не исключение: начавшись в одном месте, пожар может распространиться на весь ЦОД, нарушить его работу и уничтожить все здание и его содержимое. Большинство коммерческих зданий оснащено системами пожаротушения на основе воды, которые способны потушить пожар до того, как он нанесет слишком большой ущерб.

На некоторых объектах устанавливают систему пожаротушения на основе газовых огнетушащих веществ (ГОТВ), чтобы избежать повреждения водой незаменимых или очень дорогих, бесценных вещей, таких как предметы искусства, редкие артефакты и т.п. (В англоязычной литературе используется термин «чистые агенты» (clean agents), к которым относят не проводящие электричество летучие или газообразные вещества (например, инертные газы), не оставляющие следа после испарения и, как правило, не повреждающие ИТ-оборудование. – *Прим. ред.*)

В течение многих лет в основном использовались системы на основе хладона (Halon), но постепенно они по экологическим соображениям были в значительной степени заменены системами на основе инертных газов или галогенуглеводородов (*см. «Основные типы современных ГОТВ»*).

Согласно исследованию Uptime Institute, проведенному в 2017 г., более половины (54%) всех ЦОДов используют только газовые системы пожаротушения, а еще 28% оборудованы системами на основе как газа, так и воды. При этом эксперты Uptime Institute считают, что в большинстве случаев наличие двух систем пожаротушения – излишняя предосторожность. Она может даже увеличить риск в зависимости от того, какое огнетушащее вещество применяется, как спроектированы и инсталлированы системы.

Хотя только 18% респондентов, участвовавших в опросе, полагаются исключительно на водяные системы пожаротушения, в Uptime Institute полагают, что именно системы на основе воды с сухими трубами и клапанами предварительного действия (preaction) – наиболее подходящее решение для большинства ЦОДов.

За исключением, пожалуй, суперкомпьютеров, оборудование в дата-центре и само здание не так ценны, как информация, которая хранится в нем. А, по данным Uptime Institute, системы пожаротушения инертным газом, которые случайно разряжаются во время тестирования или технического обслуживания, могут повреждать жесткие диски ИТ-оборудования, увеличивая

Публикуется с разрешения Uptime Institute.

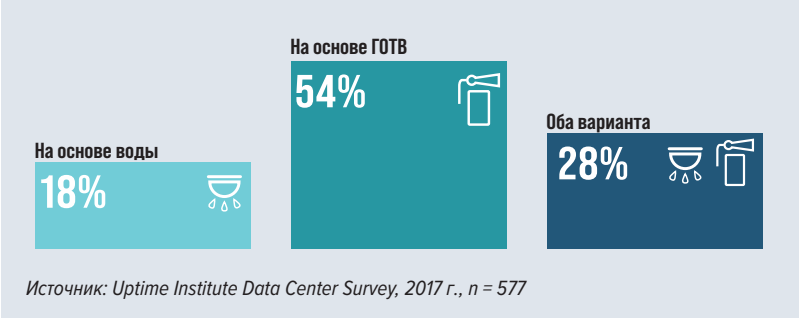
общий риск потери хранящейся в ЦОДе информации даже в отсутствие пожара. Этот риск совершенно не оправдан, поскольку, согласно исследованию 2017 г., непреднамеренные разряды систем пожаротушения в дата-центрах происходят в три раза чаще, чем пожары.

Производители ИТ-оборудования добились больших успехов в повышении его устойчивости к возможному возгоранию, однако, по оценкам Ли Кайзера, председателя комитета Национальной ассоциации противопожарной защиты США, занимающейся вопросами защиты ИТ-оборудования, примерно в 10% случаев пожар начинается именно в нем. Чуть более чем в трети случаев источником возгорания становится оборудование для распределения электроэнергии – либо в самом машзале, либо в силовом или аккумуляторном отсеке. Частым источником небольших пожаров и задымления являются ИБП. Остальные причины, например попадание посторонних предметов в ЦОД, человеческая ошибка или даже поджог, встречаются реже. При этом возгорания в машинных залах, как правило, не слишком опасны. А вот пожары, возникающие за их пределами, могут быть весьма грозными и должны быть ликвидированы с помощью соответствующих систем пожаротушения.

В связи с вышесказанным эксперты Uptime Institute рекомендуют операторам ЦОДов разработать надежный план аварийного восстановления или обеспечения отказоустойчивости бизнеса для защиты всех данных, которые считаются критическими, с использованием водяной системы пожаротушения с сухими трубами и клапанами предварительного действия. Такие системы обеспечивают надежную защиту от пожаров, возникающих в машзалах, и исключают риск повреждения ИТ-оборудования из-за непреднамеренного срабатывания.

Чтобы обезопасить себя от пожаров, операторы ЦОДов должны внимательно следить за удалением легко воспламеняющихся (огнеопасных) веществ из машзалов и других ИТ-помещений, в том числе из-под фальшполов. Горючие материалы, включая упаковку, могут стать причиной пожара или подпитывать его распространение. Обеспечение того, чтобы в помещениях ЦОДа не было легко воспламеняющихся веществ, должно быть частью стандартных процедур эксплуатации объекта.

В свое время конкуренция между коммерческими ЦОДами стимулировала использование ими газового пожаротушения – они стремились сделать свои объекты более безопасными. Но, как уже говорилось, известны несколько инцидентов, когда случайное срабатывание системы пожаротушения с инертным газом приводило к повреждению жестких дисков



Источник: Uptime Institute Data Center Survey, 2017 г., n = 577

▲ Рис. 1.
Какой тип системы пожаротушения используется в вашем ЦОДе

ИТ-оборудования клиентов. Этот риск, по-видимому, присущ исключительно системам с инертным газом, поскольку они работают при более высоком давлении, чем другие газовые системы пожаротушения.

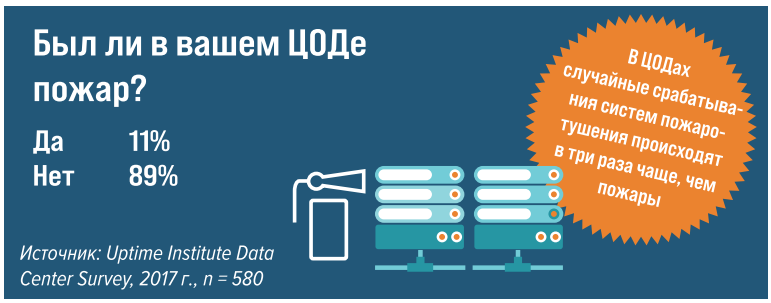
Некоторых консультантов можно обвинить в некорректном позиционировании систем газового пожаротушения для ЦОДов. Они считают такие системы более надежными, чем водяные. На самом деле этот вариант увеличивает стоимость проектирования, строительства и эксплуатации ЦОДов, не снижая риск возникновения пожара.

Типы систем пожаротушения

Чтобы оценить степень риска для ЦОДов, важно понимать различия между основными типами средств и систем пожаротушения, которые могут использовать воду, инертный газ и галогенуглеводороды, включая гидрофторуглероды (HFC) и фторкетоны.

Большинство водяных противопожарных систем распределяют воду с помощью спринклерных головок, которые расположены по всему объекту. Системы пожаротушения с сухими трубами и клапанами предварительного действия, обычно устанавливаемые в ЦОДах, используют спринклерные головки с оловянной заглушкой, которая плавится при определенной температуре, и сухие трубы под давлением, что исключает попадание воды в машзал до тех пор, пока давление не снизится. При возникновении пожара головки разбрызгивателя открываются только тогда, когда заглушки расплавятся. В этом случае давление в соответствующей трубе снижается, позволяя клапану открыться. Заглушки предотвращают попадание воды в места, расположенные по соседству

Рис. 2.
Распространенность пожаров в ЦОДах ▼



с очагом возгорания. При отсутствии пожара, даже во время тестирования и технического обслуживания, заглушка защищает оборудование от повреждения водой. Пожары, возникающие в ЦОДах, часто локальны и затухают сами, хотя объекты горения в них, как правило, находятся под напряжением. Поэтому описанные системы могут подавить возгорание, не причиняя чрезмерного ущерба оборудованию, установленному в других местах.

Эксперты Uptime Institute сознают опасность коррозии труб при попадании в них воды во время тестирования, поэтому рекомендуют заполнять их азотом для обеспечения повышенного давления в системе.

Галогенуглеводороды и инертные газы (наиболее распространенные виды чистых агентов) начали использоваться в системах пожаротушения в качестве альтернативы хладону 1301 (торговое название бромтрифторметана), который постепенно выводится из употребления во всем мире из-за его разрушающего воздействия на озоновый слой. Его негативное воздействие на здоровье людей привело к тому, что многие компании добровольно от него отказались. Однако переделка систем на основе хладона 1301 для применения современных ГОТВ обходится дорого, и поэтому этот газ по-прежнему используется в некоторых системах.

Как и в случае с хладоном 1301, инертные газы и галогенуглеводороды не требуют очистки предметов после воздействия, поэтому они хорошо подходят для защиты важных или дорогостоящих предметов (например, книг, картин, предметов культурного наследия), которые были бы уничтожены другими огнетушащими веществами. По утверждению поставщиков систем пожаротушения, эти средства не вызывают ни коррозии, ни нарушения проводимости и не повреждают электрические цепи.

Для объектов, не связанных с ИТ, системы с инертным газом и галогенуглеводородами работают также хорошо. Однако, в отличие от систем на основе воды, они заполняют весь машзал или другое помещение, где произошел пожар, а не только несколько стоек или шкафов. Эти ГОТВ должны оставаться в помещении достаточно долго, чтобы предотвратить повторное возгорание. Даже при небольшом пожаре не может быть локального воздействия. А заправка систем с ГОТВ может стоить весьма дорого.

Большая часть новых ГОТВ не токсична и, как правило, может использоваться в помещениях, где находятся люди. В сочетании со средствами раннего обнаружения системы пожаротушения на базе галогенуглеводородов и инертных газов очень эффективны: они целиком заполняют защищаемую зону, быстро туша даже труднодоступные очаги возгорания, в том числе внутри шкафов или под фальшполом. Эти системы применимы к пожарам классов A, B и C (горение твердых, жидких и газообразных веществ соответственно. – *Прим. ред.*).

Высокое давление, шум и серверы

Галогенуглеводороды в системах пожаротушения хранятся в виде сжатых сжиженных газов под давлением до 25 или 40 бар, за исключением FE-13, который представляет собой жидкость, хранящуюся при более низком давлении. Инертные газы поставляются в газовых баллонах высокого давления, обычно под давлением 200 или 300 бар (4400 psi), поэтому с ними необходимо обращаться очень осторожно. Согласно имеющимся данным, пиковое давление такого вещества может быть достаточным для того, чтобы повредить инфраструктуру дата-центра, даже стены, если помещения спроектированы неправильно и отсутствует надлежащая вентиляция.

ОСНОВНЫЕ ТИПЫ СОВРЕМЕННЫХ ГОТВ

Некоторые из перечисленных ниже наиболее популярных газовых огнетушащих веществ могут быть доступны под разными торговыми названиями у разных поставщиков.

Галогенуглеводороды

Гидрофторуглероды (Hydrofluorocarbon, HFC)

- HFC-227ea (FM-200)
- HFC-125 (FE-25)
- HFC-23 (FE-13)

Фторкетоны

- FK-5-1-12 (Novec 1230, хранится в жидком виде)

Novec 1230, по данным компании 3M, относится к семейству химических веществ, называемых галогенуглеродами. Он является заменителем хладонов и альтернативой гидрофторуглеродам (HFC). Потенциал глобального потепления (GWP) Novec 1230 – менее единицы, в то время как для HFC он превышает 3000. Жидкость Novec 1230 наиболее безопасна для людей среди всех чистых агентов.

Инертные газы

- IG-55 (аргонит)
- IG-541 (инерген)
- IG-100 (азот)
- IG-01 (аргон)

Системы с инертным газом и гидрофторуглеродами (HFC) тушат пожары совершенно разными способами. При срабатывании по сигналу датчика пожара, задымления или другого источника информации система подачи инертного газа под высоким давлением выделяет достаточное количество ГОТВ, чтобы содержание кислорода в помещении упало ниже 14,3% (типичное значение 12,5%) и дефицит кислорода привел к затуханию огня. HFC-газы низкого давления, такие как HFC-227ea, HFC-125 и FK-5-1-12, могут тушить пожары за счет поглощения тепла, поскольку обладают высокой теплоемкостью.

Инертные газы, выходящие под высоким давлением в закрытых помещениях, например машзалах, могут повредить жесткие диски серверов. Это может произойти при срабатывании системы пожаротушения как в результате реального пожара, так и из-за человеческой ошибки, неисправности или ложной тревоги, вызванной, скажем, пылью. Сильные звуковые колебания (т.е. высокий уровень шума) на определенных частотах, по словам Барта Гомана, менеджера по развитию бизнеса в регионе EMEA компании 3M, вызывают вибрацию шпинделей жестких дисков, что приводит к смещению головок чтения/записи и выходу устройств из строя. Жесткие диски последнего поколения не допускают смещения более чем на 12 нм. По мере того как диски становятся все более совершенными и их компоненты упаковываются все плотнее, вероятность их выхода из строя из-за повышенного уровня колебаний возрастает.

«При этом нам не известны случаи, чтобы выход галогенуглеводородных веществ приводил к повреждению жесткого диска. Считается, что это обусловлено тем, что галогенуглеводороды обычно выпускаются при более низком давлении в форсунках и за гораздо меньшее время, чем инертные газы, и звуковые колебания при этом меньше, соответственно ниже риск возникновения вибраций в жестких дисках», – добавляет эксперт 3M.

В ходе одного инцидента, произошедшего осенью 2017 г., в результате случайного срабатывания системы пожаротушения с инертным газом во время тестирования были повреждены серверы на критически важном банковском объекте в Восточной Европе, в результате чего ЦОД был отключен на несколько дней. В другом случае также выброс из системы пожаротушения на основе инертного газа вызвал перебои в работе ИТ-оборудования. База данных отчетов об инцидентах Uptime Institute содержит еще несколько аналогичных инцидентов, которые привели к простою ЦОДов. При этом не зафиксировано ни одного случая, когда сброс галогенуглеводородов в системах низкого давления привел бы к повреждению жестких дисков, хотя в системах пожаротушения они используются в 3,5 раза чаще, чем инертные газы.

Производители серверов осведомлены об описанных проблемах, связанных с выделением инертного газа, и большинство из них считают, что сочетание высокого уровня шума и давления выводит из строя механизмы чтения-записи жестких дисков. Уровень шума, издаваемого современными системами, включая звук сигнала тревоги во время активации системы, достигает 120 дБ. Один заказчик, у которого недавно непреднамеренный выброс инертного газа в системе пожаротушения вызвал сбой в работе ИТ-оборудования, сообщил, что производители жестких дисков требуют, чтобы предельный уровень шума не превышал 90 дБ на расстоянии 2 м от диска.

Из всего вышесказанного следует, что даже если вы предпочитаете систему пожаротушения с чистым агентом, следует избегать систем с инертным газом.

Инертные газы, выходящие под высоким давлением в закрытых помещениях, например машзалах, могут повредить жесткие диски серверов

РЕКОМЕНДАЦИИ

- Эксперты Uptime Institute рекомендуют использовать в ЦОДах водяные системы пожаротушения с сухими трубами и клапанами предварительного действия.
- Системы пожаротушения на основе ГОТВ не являются необходимыми в ЦОДах, за исключением отдельных проектов, например, в суперкомпьютерных центрах.
- Вероятность непреднамеренного срабатывания систем пожаротушения с ГОТВ в три раза выше, чем вероятность возникновения пожара. Это означает, что объект скорее пострадает от срабатывания такой системы, чем от пожара.
- Было доказано, что случайный сброс инертного газа (одного из видов ГОТВ) может привести к повреждению жестких дисков ИТ-оборудования.
- Галогенуглеводородные системы низкого давления – предпочтительный вариант, когда по коммерческим или маркетинговым соображениям требуется использовать ГОТВ.

ФАКТОЛОГИЯ ИССЛЕДОВАНИЯ

При подготовке этого материала и выработке приведенных в нем рекомендаций эксперты Uptime Institute провели неформальный опрос участников Uptime Institute Network, проанализировали свою базу отчетов об инцидентах и изучили сообщения в СМИ, чтобы дополнить результаты обзора Uptime Institute Data Center Survey за 2017 г. Это исследование подтвердило, что случайное включение систем пожаротушения с инертным газом инициировало инциденты на десятках объектов, и некоторые из них привели к простою ЦОДа и/или повреждению жестких дисков.

Многие отчеты, рассмотренные Uptime Institute, недостаточно детализированы, чтобы определить тип использованного ГОТВ. Однако, когда в отчетах содержалось достаточно информации, чтобы идентифицировать систему пожаротушения, это всегда была система с инертным газом. Этот вывод согласуется с отраслевыми отчетами и утверждением компании 3M (производителя Novec 1230) о том, что галогенуглеводородные системы низкого давления не приводят к повреждению дисков.

Эксперты Uptime Institute отмечают, что системы с современными ГОТВ имеют свои преимущества, но операторы ЦОДов должны соразмерять эти выгоды с более высокой стоимостью и тем фактом, что пожары в серверных помещениях происходят редко.

Заключение

Как показывает исследование Uptime Institute, пожары в ЦОДах происходят относительно редко, обычно вызваны ненадлежащей деятельностью человека в ИТ-помещениях или неполадками в системах электропитания и, как правило, затухают сами. Другие типы пожаров распространяются на ЦОДы из соседних помещений. В настоящее время очевидна потребность в эффективной системе пожаротушения, которая должна обеспечивать безопасность людей, защищать дорогостоящее оборудование и критически важные данные. Однако системы пожаротушения с инертным газом могут повредить объект и серверы, создавая риски для работы ЦОДа при непреднамеренном срабатывании во время тестирования и технического обслуживания.

Выбор и проектирование системы пожаротушения должны соответствовать потребностям бизнеса и рискам, с которыми может столкнуться предприятие. Водяные системы пожаротушения при работе выводят из строя чувствительное ИТ-оборудование. Однако в целом потеря ИТ-оборудования при пожаре приемлема даже для страховых компаний, которые рассматривают оборудование как заменяемое, а приоритет отдают спасению жизней и сохранению зданий. В некоторых случаях страховые компании могут даже потребовать использования системы на водяной основе. Операторы ЦОДов, возможно, не разделяют эту точку зрения, поскольку оборудование обошлось им в миллионы долларов, а хранящиеся на нем данные могут быть вообще бесценными.

Системы с современными ГОТВ лучше защищают ИТ-оборудование, поскольку они не повреждают электрические схемы даже при работе с полной нагрузкой. Кроме того, такие системы способны эффективно подавлять очаги возгорания, в том числе внутри шкафов или под фальшполом. Другим вариантом являются водяные системы, но с сухими трубами и клапанами предварительного действия, которые исключают ложное срабатывание и подают воду только тогда, когда что-то точно начинает гореть.

Системы пожаротушения с ГОТВ требуют, чтобы помещение было хорошо герметизировано. Это необходимо для того, чтобы реагент не выходил из помещения через какие-либо отверстия. Он должен оставаться в помещении достаточно долго, чтобы предотвратить повторную вспышку пожара и обеспечить аварийным службам достаточное время для реагирования.

Использование систем с высоким давлением в условиях ЦОДа сопряжено с дополнительным эксплуатационным риском. При повреждении клапана емкости с газом струя может пробить стену, покалечить или даже убить обслуживающий персонал, оказавшийся на ее пути.

Эксперты Uptime Institute считают, что невысокий риск возникновения пожара в помещении ЦОДа делает водяные системы пожаротушения с сухими трубами и клапанами предварительного действия предпочтительными для большинства объектов. Решения с современными ГОТВ могут использоваться для защиты бесценного или незаменимого оборудования или при наличии специальных бизнес-требований. ИКС

Есть ли будущее у многопарных LAN-кабелей?

Многопарные конструкции при построении СКС применяются в основном для создания телефонной сети на предприятиях. По мере того, как IP-телефония в офисах постепенно вытесняет классическую, они будут использоваться все меньше, но в среднесрочной перспективе не исчезнут вовсе.

Андрей Семенов, профессор, МТУСИ

Структурированные кабельные системы (СКС), образующие физический уровень информационно-телекоммуникационных систем (ИТС), стали сегодня таким же элементом инженерного оборудования, как водопровод, канализация, сети электроснабжения и т.д.

Современные внутриофисные СКС имеют высокую плотность портов и обслуживают также многочисленные устройства цифрового потолка. Это ощутимо удорожает внутриобъектовую информационную проводку, на которую приходится значительная доля общей стоимости ИТС. Основным объектом стоимостной оптимизации СКС является горизонтальная подсистема: на нее тратится примерно 85% всех ресурсов, выделяемых на реализацию проекта. Главное направление стоимостной оптимизации магистральных уровней проводки – отказ от соблюдения в этой части СКС принципа полной универсальности. Такой подход целесообразен, поскольку дальность передачи в них по сравнению с горизонтальной подсистемой существенно больше, а в узловых точках информационной инфраструктуры возможна эффективная селекция трафика разных приложений. Причем имеется техническая возможность мультиплексирования трафика отдельных, в первую очередь высокоскоростных приложений.

При существующей структуре затрат дальнейшая оптимизация проводки за счет применения к магистральным подсистемам принципов, работающих на уровне горизонтальной подсистемы, не даст значимого эффекта. Для решения этого вопроса нужно искать другие подходы.

Особенности построения магистральных уровней СКС

СКС как продукт массового применения гармонизируется с основными потребителями ее ресурсов, а именно локальной вычислительной и телефонной сетями предприятия. Остальные системы, входящие в состав ИТС, значительно уступают им по суммарному количеству терминальных устройств (см. таблицу) и по объему генерируемого трафика.

Управляемые через ИТС системы светодиодного освещения, которые отличаются большим количеством портов из-за высокой плотности расположения светильников, за океаном пользуются большой популярностью. Однако они оказывают исчезающе малое влияние на магистральные уровни СКС, поэтому в дальнейшем анализе их можно не принимать во внимание.

ЛВС и телефонная сеть используют технологии передачи данных, которые в общем случае несовместимы ни по аппаратуре, ни по форматам линейных сигналов. В первом случае задействована волоконно-оптическая техника, а во втором – симметричные кабели категории не выше 5e. Плюс к этому телефонная сеть должна поддерживать работу ранее выпущенных учрежденческо-производственных АТС (УПАТС). Поэтому в СКС первых поколений магистральные подсистемы делились на две основные части. При этом «телефонная» составляющая была жестко специализированной, а волоконно-оптическая использовалась другими сетями из-за их построения на основе технологии Ethernet.

Многопарные кабели и их роль при построении СКС

Многопарный кабель может выполняться по традиционной (рис. 1 а) и так называемой многоэлементной (рис. 1 б) схеме. Последняя конструкция фактически представляет собой сборку горизонтальных кабелей, объединенных в единую структуру дополнительной внешней оболочкой или обмоткой скрепляющими лентами.

Система ИТС	Количество портов
ЛВС и телефония	250
Светодиодное освещение	370
СКУД, видеонаблюдение, оповещение	12
Точки доступа Wi-Fi	4
Инженерное обеспечение	8
IP-часы, интерком и пр.	16

◀ Среднестатистическое количество портов отдельных систем ИТС в одноэтажном офисе общей площадью 1500 м²

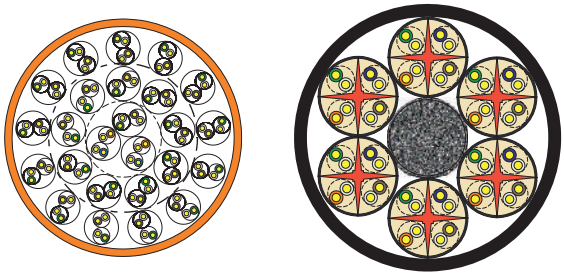


Рис. 1. Варианты исполнения многопарного кабеля по классической (а) и многоэлементной (б) схеме ▶

При реализации ИТС в офисах классические многопарные конструкции применяются для построения той части магистрали, которая обслуживает потребности телефонной сети предприятия, созданной по классическим принципам. До 2017 г. их использовали также в горизонтальной подсистеме СКС, устанавливаемой в открытом офисе. Ограниченность такой практики определялась в первую очередь сложностью монтажа из-за уменьшенных запасов по параметрам NEXT и RL, важных для качества функционирования сетевых интерфейсов.

Действующие в настоящее время редакции стандартов требуют применения на уровне горизонтальной подсистемы кабельных трактов класса не ниже E, т.е. их построения на элементной базе категории 6 и выше. Такие многопарные конструкции могут быть реализованы только в многоэлементном варианте, хотя они заметно дороже и трудозатратнее в монтаже из-за малой гибкости и сложности разделки.

В современных жилых зданиях многопарные кабели закладываются в состав вертикальной магистрали от распределительного узла до этажной коробки с прицелом использования для подачи интернета в квартиры. Такое решение, в частности, практикуется в Москве при строительстве жилых домов по программе реновации.

Принципы построения внутренней телефонной сети

Сложившиеся подходы к построению СКС позволяют получить структуру, близкую к оптимальной, и удешевить ее можно только изменением принципов построения ИТС. Одно из направлений – отказ от применения в составе магистральной части информационной проводки симметричных электропроводных кабелей. Это тем более перспективно, что цены на медь растут уже много лет и нет даже признаков замедления этого роста.

Отказаться от симметричных кабелей на магистральных уровнях СКС можно только при наличии технической возможности передачи телефонных сигналов по волоконно-оптическим кабелям. При этом надо принять во внимание два очевидных положения:

- создание внутренней телефонной сети предприятия с помощью выносов и/или организации подстанций экономически невыгодно из-за небольших расстояний и малого по сравнению с сетями общего пользования количества обслуживаемых абонентов;
- современные ЛВС имеют большие резервы пропускной способности и способны передавать дополнительный телефонный трафик без ухудшения качества функционирования сети.

При построении телефонной сети предприятия могут одновременно применяться аппараты трех разновидностей: аналоговые, цифровые и IP-телефоны. Наиболее распространенные варианты построения телефонной сети предприятия с использованием этой терминальной техники показаны на рис. 2.

Объединение телефонных аппаратов разных типов в единую систему для взаимодействия друг с другом при обычной и конференц-связи выполняет УПАТС, которая берет на себя функции центрального узла. Подключение к станции осуществляется через специализированные платы, каждая из которых обслуживает 8–32 аппаратов, рассчитана на конкретную разновидность телефонов и играет роль конвертора интерфейсов.

Аналоговые и цифровые телефоны подключаются к интерфейсным платам УПАТС по обычным или составным симметричным трактам.

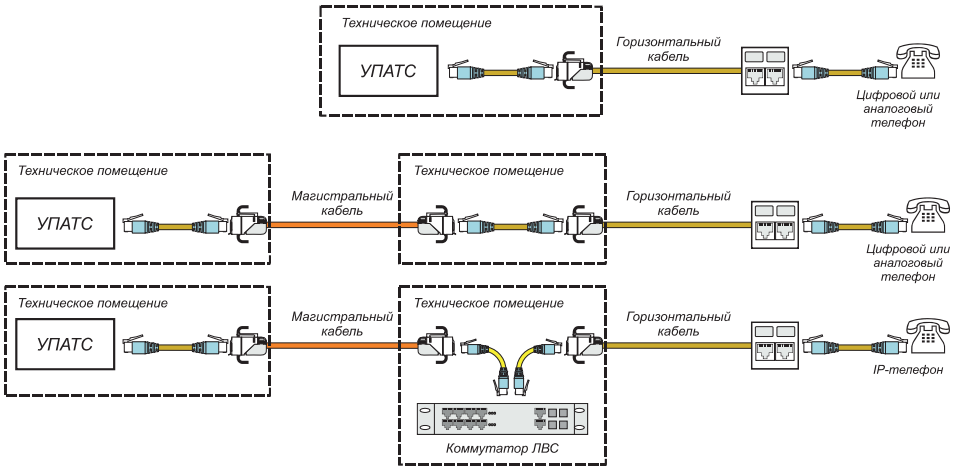


Рис. 2. ▶
Варианты построения телефонной сети предприятия.
Сверху вниз:
при централизованной структуре и классической телефонии;
при иерархической структуре и классической телефонии;
в случае применения IP-телефонии

Сигналы же IP-телефонов передаются по ЛВС, а вопрос с задержками решается применением системы приоритетов и механизмов группы QoS, т.е. на программном уровне. Коммутатор дополнительно берет на себя следующие функции:

- конвертора интерфейсов, освобождая от выполнения этой функции интерфейсные платы УПАТС;
- мультиплексора, что уменьшает требуемое количество посадочных мест в крейтах или стативах;
- преобразователя среды при необходимости передачи сигналов по волоконно-оптическим трактам.

В настоящее время широко применяются все три разновидности телефонов. Доля IP-телефонов оценочно составляет 55%, цифровых телефонов – 30%, а аналоговых – 15%, причем за последние 10 лет доля IP-телефонов, увеличиваясь в среднем на 2–2,5% в год, выросла почти вдвое. При таких темпах IP-телефония полностью вытеснит из офисных ИТС классическую телефонию примерно через 45/2,5 = 18 лет. Одновременно с этим практически полностью исчезнет необходимость использования в СКС многопарных кабелей.

Практическая потребность в многопарных кабелях СКС

Из приведенных выше выкладок можно сделать вывод, что потребность в таком специализированном продукте, как многопарный кабель, достаточно невелика и в обозримой перспективе продолжит снижаться. Это обусловлено изменением подходов к построению той части ИТС, которая предназначена для поддержки функционирования телефонной сети предприятия.

Падение интереса к классическим многопарным конструкциям при построении СКС отчетливо проявляется уже сейчас. Некоторые отечественные производители и дистрибьюторы исключают их из своего портфолио из-за малой востребованности. Такой шаг дается им тем легче, что объем применения многопарных конструкций в проектах невелик изначально.

Попробуем количественно оценить расход многопарных кабельных изделий в типовом проекте СКС с магистральной подсистемой. Влиянием подсистемы внешних магистралей пренебрежем из-за крайне малого числа проектов, в которых она присутствует.

Согласно статистике, распределение длин внутренних магистральных стационарных линий близко к экспоненциальному со средним значением 45,4 м. При проектировании телефонной части подсистемы внутренних магистралей в нее обычно закладывают 1,5 пары на одну типовую двухпортовую информационную розетку, что позволяет при необходимости эксплуатировать в составе сети системные телефонные аппараты. В расчетах целесообразно исходить из наиболее популярной на практике 25-парной конструкции. Также примем, что среднестатистическая протяженность стационарной линии горизонтальной подсистемы составляет 39,2 м.

Используя эти данные, найдем долю использования в проектах многопарного симметричного магистрального кабеля (в пересчете на стандартный четырехпарный кабель):

$$\gamma = \frac{45,4}{2 \cdot 39,2} \cdot \frac{1,5}{25} = 3,4\% .$$

Эта оценка совпадает с результатами опросов дистрибьюторов техники СКС, которые указывают, что объемы поставки многопарного кабеля в пересчете на четырехпарные конструкции составляют единицы процентов и в последние годы имеют тенденцию уменьшаться.

На фоне устойчивого снижения относительных объемов применения классических многопарных кабелей наблюдается определенный рост интереса монтажных организаций к многоэлементным конструкциям. Тому, по всей видимости, есть две причины.

Во-первых, многоэлементная конструкция позволяет без проблем получить характеристики категории 6 и неплохо востребована в открытых офисах, где на ее основе удобно формировать линейную часть стационарной линии консолидационной точки. Во-вторых, эти изделия достаточно часто применяются в многоквартирных жилых домах, они закладываются девелоперами на вертикальную магистраль в рамках программы реновации уже на стадии строительства.

■■■

Ближайшие полтора десятка лет классические многопарные конструкции продолжат применяться в проектах построения СКС, хотя внедрение в офисах IP-телефонии, которая постепенно замещает классическую, будет способствовать снижению объемов их использования примерно на 2–2,5% в год. Полного вытеснения многопарных конструкций из массовой практики реализации проектов не произойдет по крайней мере в среднесрочной перспективе, но постепенно они будут заменяться многоэлементными.

Главные факторы, которые способствуют все более широкому применению многоэлементных конструкций, – это необходимость обеспечения в горизонтальной подсистеме СКС параметров как минимум класса E (категории 6) и рост популярности открытых офисов в практике офисного строительства. ИКС

Полный текст статьи читайте на www.iksmedia.ru

EMILINK: в стремлении к технологическому суверенитету и лидерству в ЦОДах

Фокусируясь на комплексных решениях для корпоративных СКС и инженерной инфраструктуре дата-центров, максимально локализуя производство в России, ГК EMILINK намеревается обеспечить себе технологическую независимость и в ближайшие годы стать лидером на рынке решений для ЦОДов.

Андрей Зуев,
основатель и CEO
ГК EMILINK

Виктор Чепурнов,
коммерческий директор
ГК EMILINK

Леонид Юль,
руководитель отдела
продуктового маркетинга
ГК EMILINK

Марина Белоусова,
директор по маркетингу
ГК EMILINK

«ИКС»: Какие основные тенденции вы можете отметить на российском рынке инфраструктурных решений для ЦОДов?

Андрей Зуев: Сегодня, с одной стороны, растет количество предложений от российских непроизводственных компаний, которые решили, что появился шанс захватить определенную долю рынка. Они пытаются конкурировать с проверенными временем производственными компаниями, имеющими большое число успешных проектов, но на деле только дестабилизируют рынок. В этих условиях заказчики, конечно, могут «понабивать шишки», но рано или поздно на рынке произойдет естественный отбор игроков и предложений.

С другой стороны, открылось огромное окно возможностей для поставки готовых решений из Китая. При этом следует понимать компонентную зависимость от Поднебесной: любой производитель в нашей стране нуждается как минимум в одном китайском компоненте для своего изделия. Особенно это касается высокотехнологичных решений для ЦОДов, в которых доля импортных компонентов в готовом изделии может достигать 80% и больше. Чтобы минимизировать риски, мы стремимся к техническому и продуктовому суверенитету, максимально локализуя производство в России.

Это важно и потому, что с начала 2024 г. возникли проблемы с платежами в Китай и, как следствие, увеличились сроки поставок. Возможности оплаты, разумеется, существуют, однако «живут» не более месяца, а порой и несколько дней, так как постоянно вводятся новые ограничения.

«ИКС»: Как EMILINK чувствует себя на этом рынке?

А.З.: Рынок активно трансформируется, меняются игроки, но реальные отечественные производители быстро растут – и по количественным показателям, и по качественным. EMILINK целенаправленно продвигает свои топовые решения для ЦОДов и демонстрирует хорошую динамику: объем продаж к октябрю 2024 г. превысил прошлогодние показатели на 60%. По итогам календарного года мы рассчитываем довести этот рост до 80–90%.

Компании, которые еще до 2022 г. специализировались на решениях для ЦОДов, благодаря своей многолетней экспертизе получили большую фору перед теми, кто впервые вышел в эту нишу. Тот, кто сфокусировался на определенном сегменте и не распыляет силы, неоправданно расширяя ассортимент и рынки сбыта, имеет сейчас отличные возможности упрочить свои позиции и в ближайшие годы стать лидером.

«ИКС»: Какие основные события произошли за последнее время в EMILINK?

Виктор Чепурнов: В рамках стратегии развития компании поставлено сразу несколько задач, объединенных одной главной целью – упрочить лидерские позиции на рынке ЦОДов, предоставляя качественные продукты. ГК EMILINK участвует в ряде госпрограмм, направленных на оптимизацию производственных процессов и повышение качества выпускаемых товаров. Сотрудники компании проходят обучение по программе «Основы бережливого производства».

Для производства ключевые задачи текущего года – увеличение объема выпуска продукции, повышение производительности при имеющихся ресурсах и культуры производства, прямо влияющей на качество. При этом задачи по расширению номенклатуры не отошли на второй план. В конце прошлого года были введены в строй новые координатно-пробивные, лазерные и гибочные станки. В начале года в Костроме запущено производство блоков распределения питания (БРП), и уже в середине года на эти изделия был получен сертификат Минпромторга. Также с начала года мы стали выпускать шкафы высокой плотности ODF PROF, которые получили национальную премию «ЦОДы РФ» в номинации «Лучший отечественный про-

дукт». Исторически первым направлением работы компании было производство оптических патч-кордов, а с начала 2024 г. запущено производство медных.

Если говорить о результатах в цифрах: выпуск медных и оптических патч-кордов увеличен до 350 тыс. шт./мес., оптического кабеля различных конструктивов – до 190 тыс. км/год, шкафов для ЦОДов – до 1500 шт./мес. с возможностью увеличения выпуска на 30–40%, открыты дополнительные мощности для производства MTP/MPO-решений.

В качестве отдельного и важного направления развития хочется отметить запуск сертификационных курсов по СКС NTSS. При успешном прохождении квалификационных тестов по итогам курса партнерам предоставляется возможность ставить объекты на системную гарантию сроком до 25 лет.

«ИКС»: Согласно «Карте вендоров ЦОД», составляемой iKS-Consulting, вы занимаете лидирующие позиции в таких сегментах, как СКС и ИТ-шкафы. Как развиваются другие продуктовые сегменты?

Леонид Юль: Наше положение на карте вендоров связано не только с качеством серверных шкафов серии ПРОЦОД, но и с активным развитием линейки БРП. Сейчас мы предлагаем полный спектр БРП – от базовых горизонтальных моделей до современных вертикальных моделей с мониторингом и управлением, и эти решения востребованы на рынке ЦОДов. Кроме того, имея собственное производство оптического кабеля и патч-кордов, мы стараемся создавать гибкую СКС с современными решениями для офисов и ЦОДов. Очевидно, наши усилия не пропали даром, раз мы получили столь высокую оценку рынка.

Несмотря на большие амбиции, ГК EMILINK не объявляет об открытии новых линеек, пока не убедится в полной готовности направления, сервисной поддержки и активной складской программы. Мы отвечаем за свои обещания и не хотим подводить партнеров. В сентябре мы запустили направление ИБП в формате крупноузловой сборки на своей производственной площадке в России, поддерживаем наличие источников на собственных складах и у дистрибьюторов, готовы оказывать услуги по пусконаладочным работам и гарантийной поддержке.

«ИКС»: В чем сильные стороны EMILINK как отечественного производителя?

Марина Белоусова: Во-первых, это четыре собственные производственные площадки в подмосковных Котельниках и в Костроме, на которых изготавливаются медные и оптические патч-корды, оптический кабель, металлоконструкции. В 2025 г. в полную силу войдет и пятая площадка – по производству пластиковых гофрированных труб и коробов. Помимо самих мощностей – сооружений, оборудования и машин, – мы гордимся сильной командой R&D. Таким образом, мы технологически, организационно и интеллектуально готовы к реализации любых задач клиента под ключ. Речь как о штучных, нестандартных позициях, так и о массовом производстве в больших объемах.

Во-вторых, мы сфокусированы на своем сегменте и умеем «держать цель». Только так – за счет выверенного портфеля и наличия узкоспециализированных экспертов – можно поддерживать репутацию и укреплять свои позиции на профессиональном рынке.

И наконец, в-третьих, в течение 2023–2024 гг. в EMILINK собралась сильная команда профессионалов из отрасли с опытом работы в крупных компаниях-вендорах, в том числе зарубежных. Такая экспертиза позволила усовершенствовать процессы в компании и привнести лучшие мировые практики.

«ИКС»: Работаете ли вы за пределами РФ, кто основные заказчики?

В.Ч.: Наша компания развивается не только в России, но и в ближайшем зарубежье. В этом году мы открыли офис в Казахстане, в Алматы, а на территории Беларуси наши интересы представляет эксклюзивный дистрибьютор «Виватех».

Пожалуй, одним из самых специфических проектов в этом году стала поставка оптической и медной СКС, которой требовался «тропический» сертификат. Проект связан с атомной энергетикой в Бангладеш.

Наши решения успешно работают во многих коммерческих и корпоративных ЦОДах. К сожалению, заказчиков не всегда можно называть. Среди публичных проектов 2024 г. – поставка шкафов и СКС компании Freedom Finance Armenia; оптической и медной СКС в Юникредит Банк; шкафов, БРП и СКС в Центр по обеспечению деятельности Казначейства России; климатических шкафов – в телерадиокомпанию «Одинцово» и др.

«ИКС»: Каковы ваши планы по маркетинговой стратегии, по новым продуктам?

М.Б.: Наша специализация сохранится и углубится – это комплексные решения для построения корпоративных СКС, инженерной инфраструктуры серверных комнат и ЦОДов. Новые линейки и продукты ожидаются в следующих направлениях:

- стоечные ИБП (однофазные и трехфазные);
- климатическое оборудование;
- интеллектуальные БРП;
- кабеленесущие системы.

Мы продолжим участвовать в знаковых отраслевых мероприятиях и выставках. Такие ежегодные «смотры достижений» – это возможность демонстрировать свою мощь, быть в курсе тенденций рынка, оставаться на гребне волны технологий. Планируем «пересобрать» концепцию собственных мероприятий для партнеров и предложить абсолютно новый формат на стыке образования, соревнований и развлечений. Также расширим ассортимент наших обучающих программ для технических специалистов. А еще переедем в новый инженерно-технический центр в Москве, где расположится шоу-рум и лекционное пространство. Встречи с партнерами, во время которых можно не только обсудить сделки, но и с необходимой детализацией познакомить их с технической стороной продукции, – важная часть нашей работы.

Коммерческий open source: за и против

Анастасия Кузнецова,
руководитель группы по работе с ЦОД (отдел эксплуатации инфраструктуры и сервисов), «Онланта» (ГК ЛАНИТ)

Международные стандарты и внутренний вектор развития страны задают новые тенденции на рынке российского программного обеспечения. Коммерческие решения, основанные на открытом исходном коде, становятся все популярнее, вытесняя проприетарный софт.

Open source как путь к независимости

Программное обеспечение open source предоставляется конечному пользователю с открытым исходным кодом и позволяет разработчикам вносить изменения в зависимости от потребностей, не нарушая при этом права авторов исходного продукта. Такое ПО представляет собой прямую альтернативу проприетарному софту (ПС), который является частной собственностью компании или автора – разработчика ПО и не поддается свободному изменению и распространению и доступ к которому без лицензии ограничен.

Стоит отметить, что ПО с открытым исходным кодом делится на две категории:

- Свободно распространяемое ПО с открытым исходным кодом (free software). Слово free подчеркивает этические аспекты, возможность изучать, изменять и распространять ПО. Обычно предоставляется под лицензией, гарантирующей свободу использования и передачи исходного кода.
- Коммерческое ПО на базе открытого исходного года (commercial open source software, COSS). Исходный код открыт для просмотра, изменения и распространения, но при этом разработчики могут использовать его в коммерческих целях. Это означает, что компании могут создавать продукты на основе open source-технологий и продавать их, сохраняя при этом доступность исходного кода.

Последняя категория пользуется большей популярностью, так как дает возможность оперативно и с минимальными рисками совершить переход на новое решение.

Еще недавно идея использовать открытый код в бизнесе вызывала сомнения, но сегодня многие компании рассматривают коммерческие решения, основанные на открытом исходном коде, для внедрения в инфраструктуру и бизнес-процессы.

По данным исследования «Коммерческий Open Source в России: темпы внедрения и перспективы 2023–2025», проведенного Институтом изучения мировых рынков (ИИМР), за последний год использование ПО на базе open source выросло втрое по сравнению с предыдущим годом, а уже в 2025 г. увеличится в 8 раз от уровня 2023 г.

По сравнению с готовыми коробочными решениями open source-системы предоставляют лучший доступ к коду, а значит, к его контролю и изменению. Это особенно важно для критически значимых систем, в том числе тех, которые обеспечивают работу государственных организаций. При использовании открытого ПО отсутствует зависимость от внешнего вендора, управление системами осуществляется внутри компании и становится прозрачным. Регулярный ИБ-аудит, тестирование систем на наличие уязвимостей и другие меры безопасности позволяют минимизировать риски, связанные с open source-решениями.

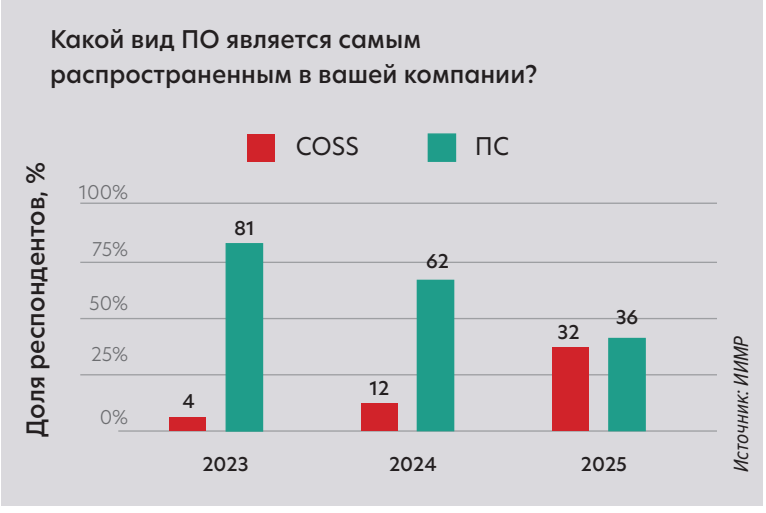
Облачная инфраструктура на базе open source

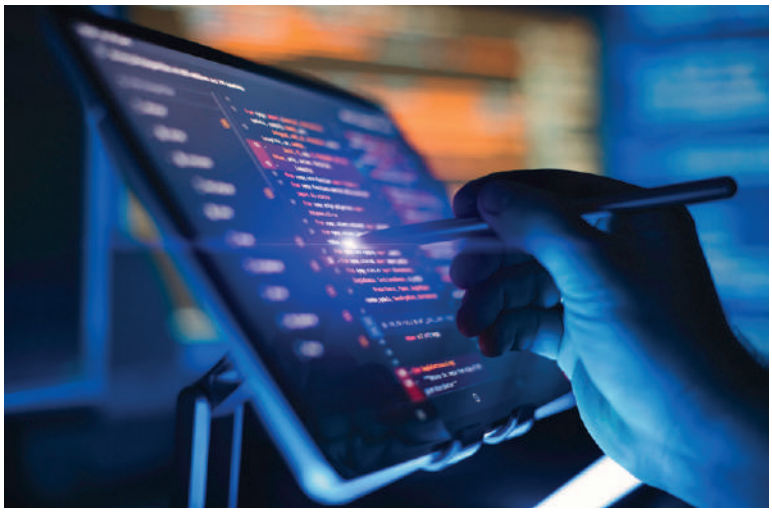
Наряду со спросом на физические дата-центры постоянно растет спрос бизнеса на виртуальные. Применение платформ виртуализации имеет ряд преимуществ перед работой исключительно на физическом оборудовании. Один из основных плюсов – возможность более эффективно использовать мощности оборудования. При переходе на технологии виртуализации компания снижает затраты на покупку нового «железа» и его обслуживание: площадку для размещения серверов, охлаждение и электроэнергию. Еще один плюс – эффективное и удобное масштабирование ресурсов как в меньшую, так и в большую сторону. Изменить параметры виртуального сервера можно оперативно, что особенно актуально для онлайн-бизнеса.

Другое немаловажное преимущество платформ виртуализации – надежность. Выход из строя физического сервера при использовании платформ виртуализации не приводит к длительному простою критически важных систем, так как их можно перенести на другое оборудование. В этом случае воздействие на конечных пользователей минимально.

Уход с российского рынка одного из крупнейших зарубежных вендоров, специализирующихся на платформах виртуализации ИТ-инфраструктуры, внес коррективы в работу облачных провайдеров и их заказчиков. Компаниям, привыкшим к стабильной и надежной поддержке вендора, пришлось заняться поиском альтернатив всей общепринятой классике систем виртуализации, сфокусировав свой взгляд на рын-

Коммерческий open source в России, 2023–2025 гг. ▼





ке отечественных решений. И, как показывает упомянутое выше исследование ИИМР, решения, построенные на открытом исходном коде, становятся все более привлекательными.

На рынке много российских решений, которые позволяют строить облачную инфраструктуру. Однако при наличии выбора всегда есть как плюсы, так и минусы.

Преимущества open source-решений

- Возможность контролировать конечный продукт или услугу – очевидный плюс использования продуктов на базе открытого кода, учитывая, что владельцы проприетарного ПО могут в любой момент изменить условия предоставления своего решения или вовсе покинуть рынок, как это случилось в 2022 г. на рынке IaaS.
- Слабая зависимость от технологий того или иного вендора. Есть возможность вносить изменения и модифицировать продукт так, как требуется бизнесу.
- При наличии решения на основе открытого исходного кода у компании появляется возможность работать с государственными организациями, предъявляющими жесткие требования к программному обеспечению.
- Ценовая политика в сфере open source более выгодная по сравнению с проприетарным ПО.
- Издержки на лицензирование коммерческих продуктов на основе открытого исходного кода ниже, чем в случае проприетарного софта.
- Использование open source-систем позволит бизнесу быстрее и безболезненнее адаптироваться в случае изменений на рынке в будущем.
- Благодаря возможности вносить изменения в код проще обеспечить совместимость и интеграцию с существующими системами.
- Решения чаще обновляются, а предложения об изменениях воспринимаются с большим интересом, так как это позволяет повысить уровень зрелости новых продуктов и лояльность их пользователей.

Открытый доступ к исходному коду может сделать open source-решение более уязвимым, поскольку злоумышленники могут изучать код для поиска слабых мест

Ограничения решений с открытым исходным кодом

- Слабая зависимость от технологий вендора. Да, этот пункт уже указан в списке преимуществ, но у монеты две стороны. Вместе со свободой изменять код по своему усмотрению мы приобретаем уникальную возможность совершать ошибки, искать их и анализировать самостоятельно. Отсутствие технической поддержки, соответствующей уровню поддержки проприетарного софта, все же является больше минусом, нежели плюсом.
- Отсутствие специалистов с нужными компетенциями. В случае с проприетарным софтом достаточно иметь в штате пару экспертов, а при использовании ПО с открытым исходным кодом появляется потребность в обширной высококлассной экспертизе.
- Необходимость переподготовки ИТ-персонала.
- Высокая стоимость перехода на новое решение. Помимо затрат на обучение, найм новых сотрудников, изменение внутренних процессов бизнес сталкивается со многими другими затратами на пути полного перехода на open source-решения.
- Ограниченный выбор аналогов уже существующих в инфраструктуре компании систем. Важный критерий выбора нового решения – сохранение, а лучше преумножение прежнего функционала и возможностей, но при сегодняшнем уровне зрелости решений на базе открытого исходного кода это скорее редкость, нежели гарантированная перспектива.
- Целенаправленная порча разработчиками собственных open source-пакетов. По данным исследования «Лаборатории Касперского», доля критических уязвимостей в таких решениях достигает 10%, опасных – 35%. Случаи порчи кода встречаются часто, поэтому с марта 2022 г. разработчики ведут список ПО с открытым кодом, создатели которого размещают в репозитории вредоносные пакеты.
- Проблема с безопасностью. Открытый доступ к исходному коду может сделать open source-решение более уязвимым, поскольку злоумышленники могут изучать код для поиска слабых мест. Поэтому важно уделять должное внимание безопасности и принимать соответствующие меры для защиты данных и систем.

■ ■ ■

Значимость open source-решений для рынка российского ПО невозможно отрицать – такие решения стремительно развиваются и используются во многих компаниях. Нужно двигаться в русле этого тренда и строить инфраструктуру с использованием open source, но не стоит забывать и про проприетарное ПО, тем самым сохраняя гибкость, актуальность и знания о передовых технологиях. ИКС

Мобильные приложения под санкциями

Очередные санкции США против российского ИТ-сектора вступили в силу 12 сентября 2024 г., и вряд ли они последние. Чем отечественный бизнес отвечает на санкционное давление?

Николай Маркашов, исполнительный директор, IW Group

Мобильные приложения банков уступают место комбинированным решениям

Санкционные ограничения существенно осложняют работу банковских мобильных приложений на iOS. Приложения российских банков, попавших под санкции, удаляются из App Store и других магазинов, пользовательские аккаунты блокируются.

Один из способов справиться с этим вызовом – перейти на веб-решения. Однако банки не спешат это делать, и не только потому, что веб-приложения более уязвимы с точки зрения информационной безопасности.

Большинство банков продолжает развивать свои прежние мобильные приложения, поскольку это не только сохраняет лояльность клиентов, но и финансово более выгодно по сравнению с запуском новых проектов. Примеры того, как банки любыми способами стараются сохранить свои мобильные приложения, показывают РСХБ, МТС Банк, Альфа-банк. Чтобы размещать свои приложения в App Store, банки делают их обезличенными, не демонстрируют свой бренд.

Мы не знаем ни одного гиганта финансовой отрасли, кто сосредоточился бы исключительно на веб-разработках. Веб-приложение для клиентов с iPhone реализует, например, Альфа-банк, но он не меньшее внимание уделяет и развитию мобильных приложений для операционных систем iOS и Android, а также для российской ОС «Аврора». Кстати, мобильные приложения для ОС «Аврора» – одно из наиболее интересных направлений корпоративной разработки для тех банков, у которых есть крупные клиенты, использующие эту операционную систему.

Комбинированная разработка действительно объединяет преимущества обоих подходов, и закономерно, что именно она сейчас завоевывает все большую популярность. Практически любое современное приложение банка представляет собой целый комплекс технологий. Ядро приложения – это, как правило, нативная разработка, а то, что не связано с финансовыми операциями, реализуется на WebView.

Новые пожелания банков к разработчикам мобильных приложений

В I полугодии 2024 г. особенно популярными у банков стали несколько видов услуг, предоставляемых разработчиками мобильных приложений.

Замена библиотек и сервисов иностранного производства на собственные решения для ОС Android и iOS. Такая замена необходима всем организациям, которые работают в сфере обслуживания населения, предоставляют критически важные услуги, в том числе финансовые, и имеют дело с персональными данными. Библиотеки и сервисы, разработанные в странах Европы и США, российские банки больше не могут использовать в принципе, а китайские аналоги слишком дороги. Приемлемые варианты для замены – российские инструменты, находящиеся в открытом доступе, либо собственные разработки.

Что выбрать, банк решает, исходя из своих потребностей. Так, в открытых приложениях для реализации мобильных сервисов могут содержаться не все функции, которые необходимы банку. Большинство банков этот мини-

мальный функционал поначалу устраивает, но прогресс не стоит на месте, и со временем банк склоняется к тому, чтобы «допилить» сервис. С библиотеками проще: российские аналоги западных решений вполне соответствуют ожиданиям клиентов.

Проекты перехода на отечественные решения реализуются достаточно быстро, иногда даже силами дочерних ИТ-структур банков, особенно у таких гигантов, как Сбер. Около месяца занимает предварительный анализ, в ходе которого заказчик выбирает необходимый функционал. Если подходящее импортозамещающее решение уже есть на рынке, то его внедрение проходит за одну-две недели. Заказная разработка займет один-два месяца в зависимости от пожеланий банка и количества библиотек. В итоге организация получает рабочее решение, которое полностью соответствует требованиям Центробанка и не вызывает вопросов у аудиторов.

Чем раньше банки проведут импортозамещение своих программных продуктов, в том числе мобильных приложений, тем больше получат конкурентных преимуществ

Модификация мобильных приложений для ОС «Аврора». Эта услуга актуальна для банков, мобильными приложениями которых пользуются сотрудники госструктур, где носимые устройства с ОС «Аврора» являются корпоративным стандартом, например, Министерства обороны или РЖД. Как правило, такие влиятельные клиенты сами инициируют модификацию мобильных приложений банков для работы с ОС «Аврора», и банк приступает к поиску разработчика, который сможет выполнить подобный проект.

Процесс модификации очень трудоемок. Например, в 2019 г. проект создания мобильного приложения на ОС «Аврора» для ВТБ занял у разработчиков почти год. В отдельных случаях, когда разработчик уже располагает необходимой аналитикой и наработками, срок проекта можно сократить до трех-четырех месяцев. Но это, опять же, будет кастомизированная разработка – единого решения, подходящего для любого банка, на рынке нет.

Развертывание собственной платформы дистрибуции мобильных приложений. Такая платформа позволяет обезопасить и самого владельца большого количества различных мобильных приложений, и его клиентов, которые этими приложениями пользуются. Если банк включен в санкционные списки, распространять его приложения в сторонних магазинах приложений рискованно. Некоторые крупные компании успешно и безопасно работают с отечественной платформой RuStore. Однако собственные платформы дистрибуции обеспечивают более глубокий контроль, анализ и управление.

Клиентский путь к сервисам банка становится удобнее и безопаснее, если у банка есть собственный магазин, где пользователи могут приобрести все мобильные решения банка. Самому банку становится проще защищать данные клиентов от вредоносного ПО, контролировать распространение приложений, делать комплексные предложения.

Допустим, у банка есть мобильные приложения для корпоративных клиентов, физических лиц, VIP, и у каждого из них своя клиентская база. Также есть приложения по отдельным продуктам и сервисам, у каждого из которых свои пользователи. Объединение клиентских баз на единой платформе открывает любому клиенту сразу весь набор услуг банка, что ведет к увеличению кросс-продаж и соответственно росту бизнеса финансовой организации. Еще одно преимущество собственного магазина мобильных приложений – возможность подключать партнеров для продаж их сервисов и более тесной коллаборации в рамках платформы.

На отечественном рынке уже есть коробочные платформы дистрибуции мобильных приложений. Банк может приобрести такую платформу по модели white label, развернуть ее на своих серверах, безопасно включить в состав инфраструктуры и организовать ролевое управление платформой. В результате риски отключения от сторонних магазинов приложений нивелируются, что положительно отражается на репутации банка.

Подготовиться к усилению санкций можно и нужно заранее

Санкции будут ужесточаться. К негативному развитию событий надо быть готовыми даже тем банкам, которые пока не попали в санкционные списки. Чем раньше банки проведут импортозамещение своих программных продуктов, в том числе мобильных приложений, тем больше получат конкурентных преимуществ. Тем более что, согласно требованиям регуляторов, к 2026 г. им в любом случае предстоит это сделать.

Кроме работающего импортозамещенного продукта банки всегда могут получить от российских разработчиков услуги сопровождения внедренного решения или помощь в обучении внутренних специалистов поддержки. В итоге решение, четко и правильно работающее в контуре заказчика, повысит безопасность сотен тысяч клиентов банка.

Печальный опыт использования иностранных решений уже получен, выводы сделаны. Было бы странно рисковать наступить на те же грабли, когда есть все возможности заблаговременно подготовить безопасную почву для дальнейшего развития бизнеса. ИКС

CLOUD & CONNECTIVITY

ФОРУМ ДЛЯ ПРОФЕССИОНАЛОВ

ИКС

18 марта 2025

Москва
офлайн + онлайн

Cloud & Connectivity – форум для тех, чья профессиональная деятельность связана с облачными технологиями и услугами, внедрением мультиклауда и гибридных ИТ-архитектур, обеспечением непрерывности и безопасности бизнеса в облачной среде.

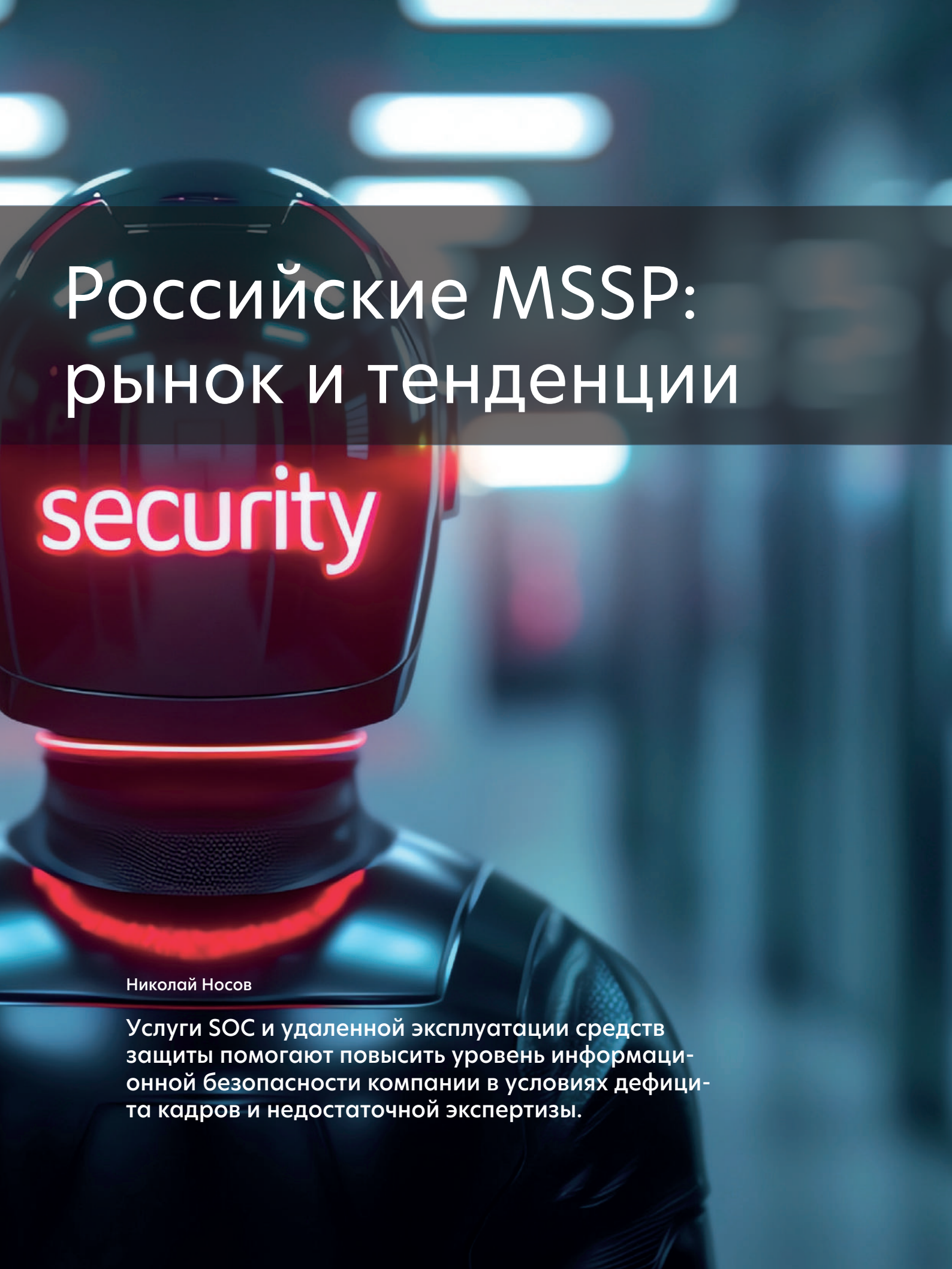
В фокусе Cloud & Connectivity 2025:

- Российский рынок облачных услуг: динамика и проблемы роста
- Связность как необходимое условие доступности и надежности облаков
- Искусственный интеллект из облака: преимущества и особенности
- Edge-облака: концепция и технические решения
- Из чего строить облака: российские платформы
- Как защитить инфраструктуру в облаках

ПРИ ПОДДЕРЖКЕ

КООРДИНАЦИОННЫЙ СОВЕТ ПО ЦОДам И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ
Автономная некоммерческая организация

CLOUDCON.RU



Российские MSSP: рынок и тенденции

Николай Носов

Услуги SOC и удаленной эксплуатации средств защиты помогают повысить уровень информационной безопасности компании в условиях дефицита кадров и недостаточной экспертизы.

Спасение утопающих – дело спасателей

В 90-е годы в московском банке, где я тогда работал, неожиданно вышел из строя выделенный канал связи с отделением, что парализовало работу филиала в Архангельске. Провайдер заявил, что у него проблем нет, наши пакеты, хоть и медленно, но доходят. Собственной экспертизы не хватило, пришлось срочно вызывать сторонних специалистов. Проанализировав трафик на сетевых устройствах, они выявили внутреннюю атаку «отказ в обслуживании» – вирус полностью занял канал с отделением, пытаясь найти доступ в интернет, чтобы связаться со своим управляющим сайтом. Зараженный сервер нашли и отключили, вирус удалили, а банк осознал важность сетевой безопасности, ведь отделение не работало, что приносило убытки.

Времена, когда на информационную безопасность не обращали внимания, а меры защиты сводились к установке антивируса, давно прошли. Бизнес понял, что ИБ – это не разовое мероприятие по закупке очередной «серебряной пули», а сложная многоплановая работа, требующая непрерывного централизованного контроля ситуации.

Для оперативного мониторинга ИТ-среды и работы систем защиты информации, а также для реагирования на киберинциденты в крупных организациях стали появляться специальные структурные подразделения – центры мониторинга безопасности (Security Operation Center, SOC). В примере с банком такой центр оперативно отключил бы подозрительное устройство. Причины проблем с сервером выясняли бы позже, но канал связи с отделением уже заработал бы и банк не простаивал.

Можно и не доводить дело до недопустимого для бизнеса события. Если за малый промежуток времени изменилось много файлов, то стоит проверить, не начал ли работать вирус-шифровальщик, который впоследствии потребует выкуп за доступ к зашифрованным данным. Если обнаружился нетипичный интернет-трафик, то, возможно, в системе появился бот, использующий вашу инфраструктуру для организации DDoS-атаки.

Сильно размыла периметр безопасности пандемия COVID-19, сделавшая удаленную работу нормой. Риски выросли, но иметь собственный SOC могли позволить себе только самые крупные компании – из-за дороговизны и острого дефицита квалифицированных специалистов. Услуги сетевой безопасности (Managed Security Services, MSS) начали отдавать на аутсорсинг провайдерам (Managed Security Service Providers, MSSP), что привело к развитию рынка сервисов информационной безопасности: услуг SOC и удаленной эксплуатации средств защиты.

Рынок MSSP в мире и в России

Передача обеспечения сетевой безопасности на аутсорсинг отнюдь не новация. Первым провайдером MSS стала американская компания US West, которая еще в 1997 г. начала предлагать клиентам использовать ей принадлежащий и ею управляемый файрвол – Check Point Firewall-1. В дальнейшем спектр предлагаемых услуг расширился, специалисты провайдера контролировали и администрировали не только файрволы (FW, NGFW, UTM), но и системы обнаружения и предотвращения вторжений, агентов для сбора и автоматического анализа информации о событиях безопасности (Security Information and Event Management, SIEM), шлюзы безопасности для почтового и веб-трафика, а также анализировали журналы безопасности, сканировали активы заказчика на уязвимости и защищали его от DDoS-атак.

Компании оценили преимущества аутсорсинговой модели при обеспечении безопасности и стали отдавать на откуп провайдерам услуг все больше сервисов. В 2019 г. Gartner относила к MSS круглосуточный удаленный мониторинг событий безопасности; администрирование и управление ИБ; обеспечение безопасности с помощью удаленных SOC. Аналитики отмечали, что основная услуга большинства MSSP – мониторинг событий безопасности и реагирование на них при обнаружении угроз, прежде всего с помощью удаленных SOC.

В список дополнительных услуг вошли:

- администрирование средств безопасности и управление файрволом, унифицированное управление угрозами, обнаружение и предотвращение вторжений, обнаружение вредоносной активности на конечных точках и реагирование на них (Endpoint Detection & Response, EDR), использование комплексной платформы защиты конечных точек (Endpoint Protection Platform, EPP), а также шлюзов безопасности для почтового и веб-трафика;
- реагирование на инциденты;
- оценка уязвимостей и управление уязвимостями (например, сканирование, анализ и рекомендации/устранение);
- анализ угроз (например, анализ машиночитаемых каналов, мониторинг даркнета для конкретных клиентов и социальных сетей);
- управляемое обнаружение и реагирование (Managed Detection and Response, MDR). MDR включает в себя EDR, а также обнаружение вредоносной активности в сетевом трафике и реагирование на нее (Network Detection and Response, NDR), совместное применение EDR и NDR, использование решений EPP и SIEM.

Если за малый промежуток времени изменилось много файлов, то стоит проверить, не начал ли работать вирус-шифровальщик, который впоследствии потребует выкуп за доступ к зашифрованным данным

Крупнейшие по выручке мировые игроки MSSP в 2023 г. ▶

	Мировые провайдеры	Страна/ Штаб- квартира	Выручка 2023, € млн
1	Thales	Франция	2400
2	Orange Cyberdefense	Франция	1100
3	Telefonica Tech	США	751
4	Rapid7	США	719
5	ECS Tech	США	693
6	Optiv	США	664
7	Ensign InfoSecurity	Сингапур	292
8	Dbappsecurity Co.	Китай	284
9	eSentire	Канада	146
10	sirar by stc	Саудовская Аравия	145
11	Kudelski Security	Швейцария	110
12	mnemonic	Норвегия	103
13	ISH Tecnologia	Бразилия	87
14	DYOPATH	США	79
15	Solar	Россия	75

Источник: iKS-Consulting

Сформировался мировой рынок MSSP, который, согласно исследованию «iKS-рейтинг. Рынок MSSP в мире: итоги 2023», проведенному аналитическим и консалтинговым агентством iKS-Consulting, возглавляют французские компании Thales и Orange Cyberdefence (см. таблицу), до 2022 г. предлагавшие услуги и на российском рынке.

На 15-м месте в этом списке – российская ГК «Солар», которая лидирует на отечественном рынке (30%). Без учета внутригрупповой выручки «Ростелекома» выручка «Солар» на рынке MSSP составила 6,9 млрд руб.

Российский рынок SOC, по оценке iKS-Consulting, в 2023 г. составил 22,9 млрд руб. В основном его формируют специализирующиеся на рынке кибербезопасности игроки, такие как «Солар», BI.ZONE, «Информзащита», Innostage, «Инфосистемы Джет». Следует также упомянуть компании Angara SOC и Qrator Labs, которая выступает и как вендор, и как MSSP (выручка за 2023 г. – 1,4 млрд руб.). Кроме того, заметны телеком-операторы (МТС RED, «Мегафон»), которым тоже интересен этот рынок. Стоит отметить интерес к рынку и у компаний, воспринимаемых как поставщики аппаратных решений кибербезопасности: весной 2024 г. предложила рынку услуги SOC компания UserGate.

Среди российских MSSP и вендоров решений для SOC отметим Positive Technologies и «Лабораторию Касперского», продукты которых активно используют лидеры рынка, а также компанию «Вебмониторэкс», чьи системы расширяют функционал SOC.

Услуги MSSP востребованы на рынке. Так, компании «Солар» и BI.ZONE обеспечивают защиту более 200 тыс. конечных точек каждая. В оказании помощи клиентам у «Солар» задействовано более 800 экспертов, более 200 работают в BI.ZONE, более сотни – в МТС RED и в компании «Инфосистемы Джет». В общей сложности «Солар» обрабатывает более 200 млрд событий в сутки, сервис BI.ZONE TDR – более 250 тыс. «сырых» событий кибербезопасности в секунду, которые в 2024 г. в результате срабатывания правил корреляции ежемесячно генерировали в среднем 26 тыс. подозрений на инциденты (так называемых алертов), анализируемых специалистами компании. За 2023 г. компания «Инфосистемы Джет» обработала не менее 50 тыс. подозрений на инциденты, «Лаборатория Касперского» проанализировала около 431 тыс. событий безопасности, примерно 32 тыс. из которых

Александр Луганский,
менеджер по развитию, UserGate

> Мы вышли на рынок коммерческих SOC только весной и пока в значительной степени находимся на этапе тестирования и пилотирования своих услуг. Однако важно отметить, что наш коммерческий SOC – это не просто сторонний сервис, который мы поддерживаем. В первую очередь эксперты центра обеспечивают нашу собственную безопасность. Они тесно взаимодействуют с нашими инженерами и аналитиками, которые постоянно изучают ландшафт угроз и внедряют защитные механизмы в наши продукты. То есть на рынок мы вышли, уже обладая опытом.

оказались следствием около 14 тыс. инцидентов. Более 120 млрд событий ежемесячно обрабатывает SOC МТС RED.

Тенденции рынка SOC/MSSP в России

Опрошенные «ИКС-Медиа» руководители компаний, активно работающих на рынке MSSP, выделили целый ряд тенденций развития этого рынка:

- рост спроса со стороны заказчиков;
- появление новых игроков – вендоров, операторов связи и облачных провайдеров;
- усиление импортозамещения;
- развитие гибридных моделей;
- появление новых направлений;
- внедрение новых технологий;
- повышение удобства работы с сервисами.

Рост спроса

В сложной геополитической обстановке, когда мир балансирует на грани полномасштабной кибервойны, риски увеличиваются и спрос на сервисы кибербезопасности постоянно повышается. О защите начинают задумываться все больше и больше компаний, в том числе те, которые раньше этого не делали. Растет потребность в экспертизе и специалистах, а они и без того в дефиците. Поэтому компании все чаще обращаются к внешним SOC/MSSP, и их востребованность растет и будет расти.

Владимир Дрюков, директор центра противодействия кибератакам Solar JSOC, ГК «Солар»

Мы наблюдаем явную смену тренда – мотивация хакерских атак поменялась с финансовой на политическую, злоумышленники переключились со шпионажа и кражи данных на прямое деструктивное воздействие (число таких атак увеличилось на порядок). На темной стороне формируется практически неограниченный список целей. Как следствие, во всех сегментах экономики РФ растет спрос на кибербезопасность, в том числе на реагирование и на поддержку процессов восстановления (не только в момент атаки, но и на этапе планирования и проектирования систем кибербезопасности).

Новые игроки

Выход на рынок операторов связи, вендоров аппаратных средств и других не специализировавшихся ранее на сервисах информационной безопасности компаний, например облачных провайдеров, – еще один, вполне естественный тренд растущего российского рынка MSSP.

Теймур Хеирхабаров, директор департамента мониторинга, реагирования и исследования киберугроз, BI.ZONE

Все больше и больше вендоров будут предлагать сервисы к своим продуктам, становясь сервис-провайдерами. А сервис-провайдеры, сами разрабатывающие элементы своих технологических платформ предоставления сервисов, будут пытаться превращать их в самостоятельные продукты и выводить на рынок, превращаясь таким образом в вендоров.

Аналогичную тенденцию мы ожидаем увидеть и у облачных провайдеров. Они интегрируют сервисы кибербезопасности в свои классические облачные сервисы, и функции кибербезопасности органически встраиваются и становятся частью ИТ-сервисов. Часть облачных провайдеров будут создавать и развивать свои сервисы кибербезопасности самостоятельно, а часть – в партнерстве с вендорами и MSSP. По нашему мнению, в перспективе двух-трех лет в России не останется ни одного серьезного облачного провайдера, который не интегрировал бы сервисы кибербезопасности в свои ИТ-сервисы. А для ускорения возврата инвестиций и увеличения выручки они станут не только предоставлять эти сервисы кибербезопасности пользователям своих облаков, но и будут пытаться выходить с ними на общий рынок, тем самым конкурируя с MSSP.

Импортозамещение

Освободившиеся после ухода с рынка западных игроков ниши начали занимать российские компании. Возросшие риски киберугроз подстегнули процессы импортозамещения. Переход на российское ПО энергично стимулируют регуляторы. Импортозамещение стало трендом и на рынке SOC/MSSP.

Дмитрий Ткачев, генеральный директор, Qrator Labs

Тренды рынка MSSP задает импортозамещение. Освободилось много ниш, которые успешно заполняют российские поставщики. Кроме того, происходит консолидация рынка, т.е. крупные игроки покупают более мелких, чтобы расширить свое портфолио релевантных сервисов. При этом есть соблазн быстро сделать что-то похожее на рабочий продукт и сразу выйти с ним в рынок. Поэтому, к сожалению, есть много незрелых продуктов, которые работают пока только в теории и в случае киберстолкновения неэффективны. Именно поэтому в сети осуществляются взломы и проходят нашумевшие атаки. Безусловно, у таких решений есть перспективы, и в ближайшие пять лет мы ожидаем качественный скачок в развитии продуктов.

Гибридные модели

С моделью MSSP конкурирует аутстаффинг, т.е. подход, в рамках которого внешние специалисты на объекте заказчика проводят расследования и решают проблемы информационной безопасности. Аутстаффингом можно считать приведенный в начале статьи пример приглашения внешних специалистов в банк для расследования сложной ситуации с сетью.

SOC, как правило, предоставляет стандартизированные услуги, не заточенные под особенности клиента. С другой стороны, чистый аутстаффинг с постоянным привлечением внешнего персонала не всегда возможен и экономически обоснован. Поэтому получают распространение гибридные схемы, когда MSSP не только предлагает стандартизированные услуги своего SOC, но и выделяет сотрудников для работы на площадке клиента с его системами ИБ и даже с потребляемыми по модели SECaaS сервисами безопасности из облака.

Ильназ Гатауллин, технический руководитель направления MTC RED SOC, MTC RED

> Среди крупных компаний заметна тенденция к выстраиванию защиты внутри себя. Это особенно характерно для объектов критической информационной инфраструктуры. Дефицит кадров в отрасли подталкивает их к гибридной модели, когда средства защиты устанавливаются внутри компании и информация об инцидентах не покидает ее периметра, но события ИБ обрабатывают аутсорсинговые команды экспертов с необходимым опытом и знаниями. Мы получали десятки запросов на гибридную модель предоставления сервисов центра мониторинга.

Новые направления

Современные MSS могут включать не только сервисы противодействия внешним угрозам (DDoS и таргетированным атакам), управление репутацией, киберразведку, но и защиту от утечек данных.

Также растет интерес к решениям класса deception, которые сбивают злоумышленника с толку и заставляют его ошибаться при горизонтальном продвижении к намеченной цели во внутреннем контуре жертвы. Некоторые игроки уже начали внедрять такие инструменты в свой портфель сервисов. Следом придет черед решений для защиты сред контейнеризации, которые позволят повысить качество мониторинга тех инфраструктур, где активно применяются контейнеры и контейнерная оркестрация.

Алексей Мальнев, директор по развитию сервисного и технологического партнерства, Positive Technologies

> Наибольшие перспективы имеют сервисы управления уязвимостями и уменьшения поверхности атаки, сервисы защищенной разработки, противодействие целенаправленным угрозам и киберразведка. В SaaS уже много лет растет популярность защиты ресурсов на уровне приложений. Хороший потенциал есть у сервисов межсетевого экранирования с глубокой инспекцией графика.

Новые технологии

Автоматизация затрагивает все направления развития ИТ, в частности MSS, куда активно проникают новые технологии, позволяющие уменьшить долю ручного труда, в том числе за счет применения систем искусственного интеллекта.

Сергей Солдатов, руководитель Центра мониторинга кибербезопасности, «Лаборатория Касперского»

> Использование ИИ и машинного обучения для автоматизации процессов обнаружения и реагирования на инциденты распространяется все шире. Это помогает повысить эффективность SOC и уменьшить нагрузку на аналитиков. При этом нужно помнить, что целевые атаки сейчас планируются все тщательнее, а следовательно, становятся все опаснее. Поэтому, несмотря на эффективную работу автоматизированных решений, таких как XDR или EPP, крайне важна результативная работа аналитиков SOC в рамках MDR.

Увеличивается и количество атак, и их сложность. В таких условиях компаниям необходимо пересматривать технологический стек своих SOC. «Профессиональные атаки все реже могут быть выявлены при помощи простого анализа логов и SIEM и требуют применения на защищаемом канале или объекте специализированных сенсоров – систем анализа трафика (Network Traffic Analysis, NTA), EDR, Sandbox – для эффективной обработки утилит», – подчеркнул В. Дрюков.

Эксперт отметил, что сегодня инструменты, направленные на нарушение доступности сайтов (магистральные и прикладные DDoS-атаки), эволюционируют. Атаки на каналы связи в основном нацелены на сети провайдеров, а DDoS уровня приложений все чаще мимикрируют под легитимный трафик. При этом злоумышленники готовят специализированный профиль атаки

для каждого конкретного ресурса. Все это требует совершенствования механизмов защиты и повышения уровня компетенций служб кибербезопасности.

Т. Хеирхабаров прогнозирует дополнительное оснащение SOC решениями для повышения эффективности обнаружения угроз и реагирования на них. Сейчас повсеместно внедряются решения EDR и NTA.

Удобство и гибкость

Конкуренция заставляет MSSP уделять больше внимания гибкости и удобству сервисов для заказчиков: объединению разрозненных панелей управления отдельными сервисами в единые личные кабинеты, упрощению обучения новых сотрудников, предоставлению все большего количества «ручек» для самостоятельного управления теми или иными параметрами сервисов. Кроме того, по мнению Т. Хеирхабарова, хорошие перспективы имеет введение единой подписки на несколько сервисов, в рамках которой заказчик приобретенные условные единицы может по своему усмотрению тратить на различные сервисы провайдера.

Также эксперт полагает, что все больше предложений сервисов кибербезопасности будет предназначаться для SMB. В настоящее время такие сервисы потребляют преимущественно крупные компании, а предложений для SMB практически нет.

Сегодня и завтра

Рынок SOC/MSSP достаточно быстро растет. Как уже говорилось выше, драйверы этого роста – увеличение количества и повышение «качества» (сложности и разнообразия) кибератак, а также дефицит квалифицированных кадров. Для обеспечения безопасности компании будут все чаще обращаться к MSSP.

Валерий Степанов, руководитель направления Центра компетенций по информационной безопасности, «Т1 Интеграция»

> Стабильный спрос на SOC сегодня подпитывают несколько факторов. Во-первых, SOC становятся все более автоматизированными, что позволяет быстрее обнаруживать возникающие киберугрозы и реагировать на них. Во-вторых, SOC оснащаются современными инструментами для мониторинга и анализа данных, благодаря чему угрозы эффективно выявляются не только в головной организации, но и у подрядчиков. Кроме того, использование ИИ и машинного обучения дает возможность выявлять угрозы и принимать решения в режиме реального времени.

По оценкам iKS-Consulting, рост выручки российского рынка SOC/MSSP в ближайшие годы составит 20–25%. Текущие тенденции подтверждают оптимизм аналитиков.

Будущее рынка MSSP будет определяться способностью провайдеров адаптироваться к новым угрозам, работать в различных условиях, например в контейнерных средах, использовать передовые технологии и интегрировать безопасность во все корпоративные бизнес-процессы. ИКС

Искусственный интеллект и угрозы информационной безопасности

Николай Носов

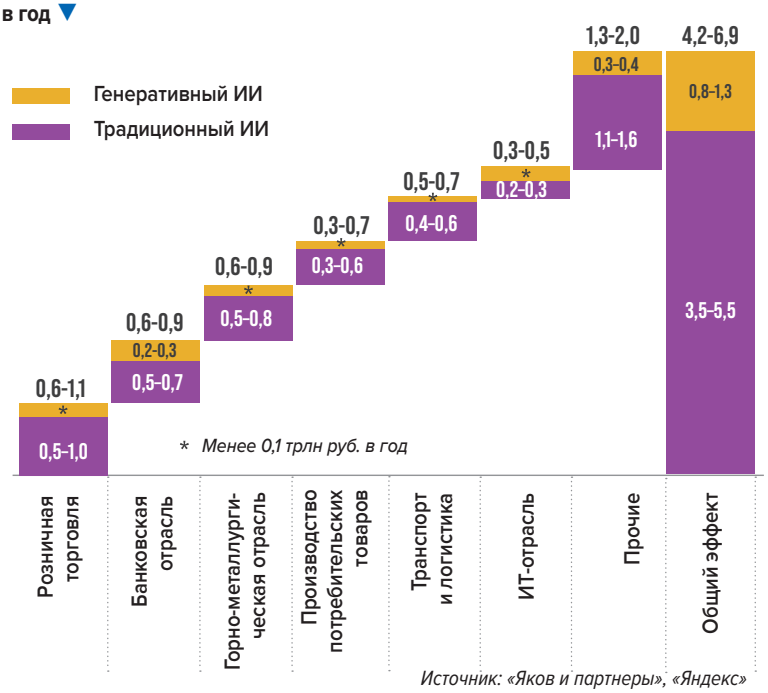
И государству, и бизнесу, да и гражданам тоже нужен доверенный ИИ, защищенный от вредоносных воздействий на всех этапах разработки и обучения, соответствующий принятым в стране этическим и правовым нормам.

Мода на ИИ

Тема искусственного интеллекта (ИИ, AI) стала самой обсуждаемой в ИТ. На вершине хайпа кривой перспективных технологий Gartner: генеративный AI (GenAI); AI-augmented software engineering – использование технологий искусственного интеллекта, таких как GenAI и машинное обучение, для помощи инженерам-программистам в разработке, кодировании и тестировании приложений; Prompt Engineering – разработка и оптимизация запросов (промптов) для эффективного использования больших языковых моделей, что привело к появлению новой специальности промпт-инженер. Подбираются к вершине AI TriSM – управление доверием, рисками и безопасностью ИИ, включающее фильтрацию и оценку подлинности контента, соблюдение ИИ-этики и законодательства; Federated Machine Learning – распараллеливание обучения и хранения данных; Reinforcement Learning – обучение с подкреплением, когда система (агент) взаимодействует со средой, параллельно обучаясь и получая вознаграждения за выполнение действий. На горизонте 10 лет просматривается Artificial General Intelligence – сильный искусственный интеллект общего назначения, который способен мыслить и действовать как человек.

На внедрение технологий ИИ возлагают много надежд. Так, совместное исследование консалтинговой компании «Яков и партнеры» и «Яндекса» оценивает эффект использования технологий ИИ к 2028 г. в 4,2–6,9 трлн руб., или до 4% ВВП. Ожидается, что пятую часть (0,8–1,3 трлн руб.) даст применение генеративного ИИ, создающего тексты, видео и изображения на основе запросов (рис. 1). Основные потребители: ритейл, банки, горно-металлургическая отрасль, производство потребительских товаров, ИТ, транспорт и логистика.

Рис. 1.
Ожидаемый финансовый эффект от внедрения ИИ, трлн руб. в год ▼



Источник: «Яков и партнеры», «Яндекс»

Новые вызовы

Новые технологии несут новые риски, в том числе в области информационной безопасности. Не исключение и технологии искусственного интеллекта. По сути мы имеем неизвестно как и кем обученный «черный ящик», результаты работы которого проверить, как правило, нельзя. При этом понятно, что по крайней мере на этапе отладки «черный ящик» будет совершать ошибки, а злоумышленники будут пытаться его обмануть или повлиять на ход его рассуждений.

Общие риски использования ИИ назывались не раз:

- этические;
- потеря рабочих мест;
- нарушение безопасности и приватности данных;
- риски для автономных систем под управлением ИИ;
- формирование зависимости от технологии;
- отсутствие ответственности;
- рост социального неравенства.

Среди ИИ-рисков советник по стратегии АНО «Национальный технологический центр цифровой криптографии» Петр Ганелин на встрече

экспертного сообщества по криптографии и большим данным, посвященной обсуждению темы «Доверенный ИИ», особо выделил риски информационной безопасности: риски, связанные с данными (ограничения, качество, утечки); атаки на ИИ и модели машинного обучения; недостаток доверия и невозможность тестирования модели; использование ИИ злоумышленниками (рис. 2).

Например, путем «отравления» данных (т.е. подачей на вход искаженных злоумышленником тренировочных датасетов) модели можно обучить нежелательному поведению, с помощью специально подготовленных анализируемых данных – обмануть или перенагрузить. А атака инверсии обученной модели может привести к раскрытию конфиденциальной информации. Все это необходимо учитывать в процессе обучения, который должен включать в себя защиту от типичных атак на нейросети.

Правонарушитель может использовать ИИ при планировании атаки или изготовлении дипфейков, в которых нейросети добились впечатляющих результатов. Так, более 50 млн просмотров набрал реалистично созданный кинематографическим ИИ студии The Dor Brothers ролик, в котором кандидаты в президенты США и другие известные люди грабят продуктовые магазины.

Риски реализуются через атаки, которые уже осуществляются и развиваются. В популярном у безопасников атласе Mitre перечислены 56 тактик атак, связанных с технологиями ИИ, из которых 14 появились в 2023 г. АНО «Национальный технологический центр цифровой криптографии» выделяет три основных класса атак: направленные на нарушение конфиденциальности, на нарушение целостности и доступности информации (рис. 3).

Нельзя сказать, что все атаки новые. В молодости в аспирантуре, занимаясь тем, что через 20 лет назовут Big Data, выявил особенность на

▲ **Дональд Трамп грабит продуктовый магазин. Кадры из ролика студии The Dor Brothers**

почти идеальном гауссовском распределении усилий при извлечении топливных сборок одного из реакторов. Распределение обрывалось резким пиком при достижении значения N. Как удалось выяснить, N – это технологически установленное предельно допустимое значение, и извлечение сборки с превышающим его усилием могло привести к обрыву троса и аварии на реакторе. За такие действия наказывали лишением премии, и персонал, чтобы не потерять деньги, указывал в отчете не реальное, а предельное значение. В результате исходные данные для моего анализа, нужные для построения многомерной модели конструкции реактора, были искажены, причем не злостными хакерами, а обычными советскими людьми – наглядный пример непреднамеренной атаки путем «отравления» обучающей выборки.

Первые «ответки»

Регуляторы разных стран начали осознавать угрозы использования ИИ и принимать меры к снижению рисков. В области законодательства лидирует ЕС. В марте 2024 г. Европейский парламент принял, а в мае Совет ЕС одобрил закон об искусственном интеллекте (Artificial Intelligence Act), который классифицирует и регулирует использование приложений на основе

Источник: АНО «Национальный технологический центр цифровой криптографии»

Рис. 2. Риски информационной безопасности ИИ ▼

Рис. 3. Классы атак на ИИ по целям атаки (по данным АНО «Национальный технологический центр цифровой криптографии») ▶

искусственного интеллекта в зависимости от риска причинить вред пользователю. Исходя из предложенной классификации, продукты ИИ делятся на три категории:

- запрещенные системы (с недопустимой степенью риска);
- системы с высокой степенью риска;
- остальные системы искусственного интеллекта.

К запрещенным практикам отнесли биометрическую категоризацию для определения сексуальной ориентации или религии, а также несанкционированное извлечение изображений лиц из интернета и записей с камер наблюдения.

Поставщики и пользователи систем с высокой степенью риска, представляющих угрозу здоровью, безопасности или основным правам человека, должны обеспечивать безопасность и соблюдение действующего законодательства на протяжении всего жизненного цикла систем ИИ. Разработчикам придется раскрывать принципы работы своих технологий и предоставлять датасеты, использованные для обучения систем.

За игнорирование запретов на определенные виды использования ИИ на компании налагается штраф до 35 млн евро или 7% годовой выручки (в глобальном масштабе, если компания транснациональная).

Безопасностью использования ИИ озаботились и в России. В Национальную стратегию развития искусственного интеллекта на период до 2030 г. указом Президента РФ от 15.02.2024 № 124 внесен пункт о необходимости обеспечения безопасности при разработке и использовании технологий искусственного интеллекта.

В мае 2024 г. при поддержке Минцифры в России создан консорциум для исследований безопасности технологий искусственного интеллекта. В числе его участников Национальный технологический центр цифровой криптографии, Академия криптографии Российской Федерации и Институт системного программирования им. В.П. Иванникова РАН.

По сути, в ИБ появилось новое направление – обеспечение безопасности ИИ, которым занимаются и научные круги, и бизнес. Так, по словам старшего аналитика группы R&D-исследований «Солар» Полины Сокол, в компании выстроена система защиты разрабатываемых моделей, охватывающая все этапы жизненного цикла ИИ-решения. Например, на этапе подготовки обучающего датасета используется кластерный анализ для выявления «ядовитых» данных. Для обеспечения конфиденциальности при хранении исходных данных помимо стандартных средств разграничения доступа применяется гомоморфное шифрование, позволяющее выполнять вычисления на зашифрованных данных без их расшифровки. При использовании open source-компонентов проводится анализ кода и проверка модели на открытых датасетах.

Востребованы и уже появились на кривой Gartner технологии защиты от дипфейков (Disinformation security). Вопросы управления доверием, рисками и безопасностью ИИ, пусть и в упрощенном виде – «роботы отнимут у нас работу, а “Скайнет” всех уничтожит», – широко обсуждаются на телевидении и в СМИ, даже далеких от техники. На уровне Госдумы рассматриваются вопросы этики ИИ, причем к обсуждению присоединилась даже церковь. Ставится вопрос о технологическом суверенитете ИИ – неизвестно, что заложено в ИИ недружественных стран и к каким последствиям приведет их бездумное использование.

Сегодня много делается для создания доверенного ПО, разрабатываемого в соответствии с концепцией жизненного цикла безопасной разработки. Точно так же нужно подходить к построению доверенных моделей ИИ. А для этого нужны совместные усилия науки, бизнеса и государства. ИКС

Dunham-Bush: комплексные решения для охлаждения ЦОДов

Стремительный рост объемов обработки данных обусловливает быстрый рост индустрии дата-центров, что, в свою очередь, повышает спрос на системы охлаждения – один из ключевых элементов инфраструктуры ЦОДов, обеспечивающих эффективную и надежную работу ИТ-оборудования.

Компания United Elements («Юнайтед Элементс») предлагает для российских дата-центров решения компании Dunham-Bush, одного из мировых лидеров в области систем охлаждения. Этот производитель выпускает всю линейку оборудования, необходимого для решения задач кондиционирования ЦОДов: все варианты холодильных машин (чиллеров) для подготовки охлажденной воды, а также широкий комплекс доводчиков – канальных, рядных, напольных, холодных стен и коридоров.

Одна из инновационных разработок компании – **чиллер Dunham-Bush DLDC-M**.

Это холодильная машина с водяным охлаждением и безмасляными компрессорами на магнитных подшипниках. Холодопроизводительность чиллера – от 250 до 3500 кВт. Решение отличает высокая сезонная эффективность и низкий уровень шума. Машина оснащена продвинутым контроллером с интуитивно понятным интерфейсом и комплексной защитой от потери электропитания.

Высокая эффективность. Достигается за счет отсутствия лишних передаточных механизмов. Крутящий момент передается напрямую с вала на рабочее колесо компрессора, и потери энергии на трение отсутствуют. Встроенный инвертор обеспечивает плавное регулирование производительности и сверхнизкое потребление энергии. Все это повышает сезонную эффективность на 30%.

Чиллер в стандартной комплектации оснащается встроенным экономайзером, который переохлаждает фреон перед испарителем, тем самым повышая эффективность холодильного цикла. Испаритель затопленного типа обеспечивает эффективную теплопередачу фреон – вода.

Быстрая перезагрузка. Для полной перезагрузки чиллера после потери питания требуется не более 180 с. Это достигается за счет подключения чиллера к ИБП, а также наличия встроенных в чиллер элементов для быстрого рестарта, которые включают в себя датчики выравнивания давления, управление насосами и охлаждением конденсатора и т.д. В итоге перезапуск компрессора занимает всего 30 с, а выход на режим 100%-ной загрузки происходит менее чем за 180 с.

Интеграция в любую систему BMS. Современные хладоцентры ЦОДов, как правило, интегрированы в общую систему мониторинга, поэтому все оборудование Dunham-Bush поддерживает все необходимые протоколы связи. Кроме того, решение Dunham-Bush имеет собственную систему комплексной автоматизации, позволяющую интегрировать в одну сеть все оборудование для охлаждения и управлять им по уникальной логике, обеспечивающей оптимизацию процессов взаимодействия.

Самый продвинутый контроллер в отрасли. Dunhum-Bush разработала контроллер DB-Vision, оснащенный сенсорной панелью управления с диагональю 10,64". Встроенная память и флеш-память позволяют сохранять все логи и данные о работе оборудования без риска утери.

Сверхнадежная система защиты. Четыре конденсатора по 8000 мкФ обеспечивают резервную мощность для поддержания левитации ротора при сбоях питания. Система датчиков контролирует положение вала каждую миллисекунду. Прецизионный контроль мощности обеспечивается в том числе за счет электронного расширительного клапана последнего поколения, который меняет расход хладагента точно под моментальные потребности.

Защита окружающей среды. Чиллеры адаптированы для использования хладагентов последнего поколения с нулевым потенциалом разрушения озонового слоя. Магнитные подшипники обеспечивают левитацию вала и уровень шума не более 73 дБ.

uel.ru

Dunham-Bush	United Elements («Юнайтед Элементс»)
Основана в 1894 г., один из старейших и ведущих мировых производителей коммерческих систем отопления и кондиционирования воздуха. Компания известна как инноватор в области компрессоростроения. Это единственный производитель винтовых компрессоров, изготовляемых по уникальной технологии – в герметичном корпусе с вертикальным расположением винта. Помимо этого, компания выпускает центробежные компрессоры всех известных модификаций, том числе уникальные безмасляные компрессоры на магнитных и газовых подшипниках.	Основана в 1993 г. За 30 лет работы на рынке вентиляции и кондиционирования реализовала свыше 6 тыс. проектов, в том числе в ЦОДах. Опыт и квалификация позволяют United Elements комплексно решать задачи охлаждения любой сложности и на любом этапе: проектирования, поставки оборудования, шеф-монтажа, пусконаладки и дальнейшего сервисного обслуживания. United Elements работает только с премиальным сегментом оборудования, поэтому качество, эффективность и долговечность эксплуатации не вызывают сомнений.

Блоки распределения питания для ЦОДов

Компания ENERGON представила блоки распределения питания (БРП) SMARTWATT PDU P-Series, предназначенные для электропитания, мониторинга и управления ИТ-оборудованием в серверных шкафах. Линейка включает 21 модель, что позволяет выбрать устройство с необходимым функционалом.

БРП поддерживают несколько протоколов безопасного доступа к данным: HTTPS, SNMP V1/V2/V2 (Trap). Устройства оснащены комбинированными розетками C39 + C13 с функцией автоматической блокировки (защитой от случайного выдергивания), а также съемным контроллером с возможностью «горячей» замены. Компактный и плоский дизайн контроллера и автоматических выключателей оставляет больше пространства в серверных шкафах.

Основные характеристики БРП:

- Мониторинг мощности подключенного устройства, полной мощности, коэффициента мощности, фазного напряжения, тока, потребленной электроэнергии и частоты, а также статуса розетки и состояния нагрузки.
- Управление отдельными розетками и группами розеток.
- Настраиваемые пороговые значения срабатывания аварийной сигнализации с доступом к сети для недопущения перегрузки цепей.
- Отправка электронных уведомлений о событиях, связанных с БРП, и системных событиях.
- Различные уровни доступа: Admin User (пользователь с правами администратора), Super User (пользователь с расширенными правами) и Read Only (пользователь с правами «только чтение»).
- Ведение журнала событий (до 400 записей).
- SNMP-ловушки (V1, V2c и V3) – в зависимости от категории системного события.
- Протоколы безопасности для аутентификации и шифрования.
- Возможность каскадного подключения до 32 БРП любого типа с использованием входных и выходных портов, поэтому требуется только одно сетевое подключение.
- USB-порт, обновление ПО и экспорт системных событий.
- Синхронизация времени с SNTP-сервером.

В ассортименте продукции есть как складские, так и заказные модели. Для заказных БРП можно выбирать материал и цвет корпуса, дизайн и компоновку розеток, тип и количество защитных устройств.

Гарантия на все оборудование – три года.

energon.ru

Мобильный ЦОД высокой нагрузки

Компания ART Engineering представляет мобильный центр обработки данных ART DLC, способный обеспечивать работу высоконагруженных ИТ-стоек.

ART DLC рассчитан на шесть ИТ-стоек с нагрузкой до 50 кВт каждая. ЦОД оборудован телекоммуникационными шкафами и PDU производства ART Engineering, а также модульным ИБП со временем автономии до 15 мин. Мобильный ЦОД может эксплуатироваться при температурах от –50 до +50°C. Конструктив имеет третью степень огнестойкости и класс пожарной опасности C0.

В ART DLC используется технология прямого жидкостного охлаждения, т.е. тепло от процессоров и графических ускорителей передается непосредственно в жидкость. В результате около 75% тепла отводится жидкостью, а оставшиеся 25% – традиционным воздушным способом (жидкостное охлаждение применяется только для тех компонентов системы, которые выделяют наибольшее количество тепла). Таким образом, системы ART DLC могут снизить потребление энергии на охлаждение, поскольку требуются менее мощные вентиляторы и компрессоры.

Мобильный ЦОД ART DLC изготавливается с преимущественным (90%) использованием отечественных материалов и комплектующих.

art-engineer.ru

Контейнерный ЦОД

Компания Protect Power Systems представила контейнерный центр обработки данных – полностью интегрированное решение на базе стандартных 20- или 40-футовых контейнеров, включающее в себя от трех (в 20-футовом контейнере) до восьми стоек (в 40-футовом) с ИТ-системами (серверы, системы хранения данных, сетевое оборудование), а также системы охлаждения, бесперебойного электроснабжения и пожаротушения.

Общая мощность ИТ-систем – 18–27 кВт (20 фт) или 48–72 кВт (40 фт). Максимальная ИТ-нагрузка на шкаф – 9 кВт.

Система электропитания строится на основе модульного ИБП с онлайн-топологией мощностью 40–90 кВА (20 фт) или 90–150 кВА (40 фт). Батареи выбираются в зависимости от проекта. Каждая стойка укомплектована двумя PDU с розетками IEC (16 или 32 А) в количестве от 16 до 42 шт.

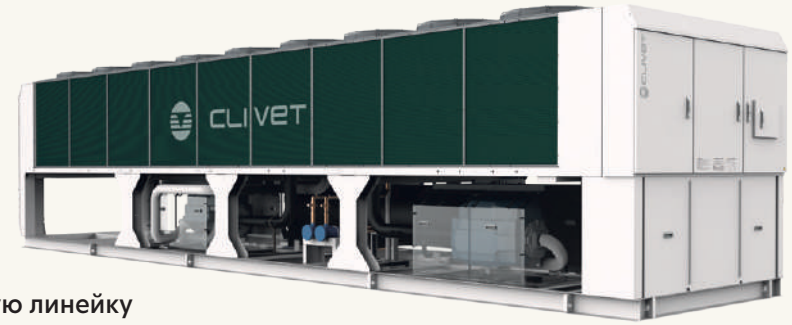
Система охлаждения по умолчанию состоит из рядных инверторных кондиционеров мощностью 25 кВт.

ЦОД оснащен системой мониторинга питания и окружения, обеспечивающей централизованное слежение за ГРЩ, ИБП, кондиционерами, системой видеонаблюдения, пожарной сигнализацией и т.д., а также СКУД и локальной индикацией. Система поддерживает световую и звуковую сигнализацию, оповещение через мобильные сети и по электронной почте. В автоматической системе пожаротушения используется тушащее вещество FM200 (опционально – Novec 1230).

Класс пыле- и влагозащиты – IP55. Рабочий диапазон температуры окружающей среды – от –40 до +50°С. При температуре ниже –20°С требуются дополнительные компоненты и обязательная изоляция трубопровода хладагента. Габаритные размеры 20-футового контейнера 2896 × 2438 × 6058 мм, 40-футового – 2896 × 2438 × 12192 мм. Нагрузочная способность 20-футового – 7 т, 40-футового – 15 т.

upsprotect.ru

Воздухоохлаждаемые чиллеры



Компания «Кливет» расширяет продуктовую линейку чиллеров с воздушным охлаждением и выводит на российский рынок воздухоохлаждаемые чиллеры на базе центробежного компрессора второго поколения с магнитными подшипниками.

Чиллеры WTAT-CNA*HV FCD имеют мощность от 285 до 1330 кВт и укомплектованы безмасляными центробежными компрессорами Midea второго поколения переменной скорости с магнитными подшипниками и цифровым управлением, а также осевыми вентиляторами с электронным управлением (EC).

Ресурс подшипников и ресурс надежности критичных узлов агрегата увеличены по сравнению с предыдущими моделями. Конденсатор имеет антикоррозийное покрытие (возможны несколько типов).

Чиллеры способны работать, в том числе в режиме свободного охлаждения (фрикулинга), при температуре до –40°С. Предусмотрена работа в смешанном режиме и режиме полного прямого фрикулинга (FCD).

www.clivet.com

РЕКЛАМА В НОМЕРЕ

Указатель фирм и организаций

Учредитель журнала «ИнформКурьер-Связь»:

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

КООРДИНАЦИОННЫЙ СОВЕТ ПО ЦОДам И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ
Автономная некоммерческая организация

АНО КС ЦОД приглашает
принять участие в практических тренингах в 2025 году

Открой новое пространство знаний о ЦОД и облачных технологиях!

- ПОСТРОЕНИЕ ЦОД
- УПРАВЛЕНИЕ ПРОЕКТИРОВАНИЕМ И СТРОИТЕЛЬСТВОМ ЦОД
- ЭКСПЛУАТАЦИЯ ЦОД
- ЭЛЕКТРИЧЕСКИЕ И МЕХАНИЧЕСКИЕ СИСТЕМЫ ЦОД
- ОБЛАЧНЫЕ ТЕХНОЛОГИИ
- ТЕЛЕКОММУНИКАЦИИ И СЕТИ В ЦОД
- НОРМАТИВНАЯ БАЗА И ПРИМЕНЕНИЕ СТАНДАРТОВ ЦОД

ОБУЧАЮЩИЙ ЦЕНТР АНО КС ЦОД

Профессиональные тренинги, разработанные совместно с ведущими экспертами-практиками рынка коммерческих и корпоративных дата-центров, охватывающие все стадии жизненного цикла ЦОДа, все ключевые системы его функционирования.

25 ТРЕНИНГОВ ✖ 615 ВЫПУСКНИКОВ ✖ 408 СЕРТИФИКАТОВ

KEY POINT GROUP

РЕГИОНАЛЬНАЯ СЕТЬ ЦОД ГРУППЫ КОМПАНИЙ KEY POINT

ВАЖЕН КАЖДЫЙ!

ДАТА-ЦЕНТРЫ С СЕРТИФИКАЦИЕЙ TIER III

Реклама

keypoint-group.ru