ИТ • Телеком • Медиа | www.iksmedia.ru | № 3 2023

ТЕМА НОМЕРА

БЕЗОПАСНОСТЬ БРЕНДА В КИБЕРПРОСТРАНСТВЕ

ИнформКурьер-Связь
ИКС
издается с 1992 года

Роман Шмаков

Первый заместитель генерального директора по рынку «ИТ-решения» и сервису, Systeme Electric

Пора возвращаться к комплексным решениям

TICA®

БОЛЬШЕ, ЧЕМ ВЫ ОЖИДАЕТЕ

Решения для ЦОДов

Чиллеры
с воздушным охлаждением
на базе спиральных
и винтовых компрессоров

Чиллеры
с водяным охлаждением
на базе спиральных
и винтовых компрессоров

Безмасляные
центробежные чиллеры
с водяным охлаждением

Безмасляные
центробежные
чиллеры с воздушным
охлаждением

Сухие охладители

Прецизионные
кондиционеры

Установки
с адиабатическим
охлаждением

Холодные стены
(FAN WALL)

Engineering Solutions

ООО «Инжиниринг Солюшенс»

Официальный дистрибьютор TICA CLIMATE SOLUTIONS в России

+7 495 120 4232
+7 812 220 1242
info@engsolutions.ru
www.engsolutions.ru

Реклама

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: 25.08.23.
Дата выхода в свет: 05.09.23.
Тираж 5 000 экз. Свободная цена.
Формат 64x84/8
Типография: ООО "ПРОПЕЧАТЬ",
адрес типографии 119618, г. Москва,
Боровское ш., дом 2А, корп. 4, кв. 260.

ISSN 0869-7973

Проблемы сервиса и масштаба

Оптимизм заказчиков относительно отечественных решений для ЦОДов все чаще сменяется некоторым разочарованием, связанным с невысоким качеством продукта. И речь даже не только, а зачастую и не столько о качестве непосредственно изделия, сколько о качестве сервиса, необходимого на всех этапах его жизненного цикла. Любая «железка» даже самого маститого мирового производителя может сломаться, но эта поломка не остановит грамотно спроектированный и построенный ЦОД. На то и избыточность, реализованная с помощью различных схем резервирования. А вот сервис ответственного производителя должен обеспечить максимально быструю замену (ремонт) отказавшего блока (модуля) или всего устройства, чтобы восстановить заложенную в проект избыточность. И над развитием сервиса нашим производителям еще работать и работать.

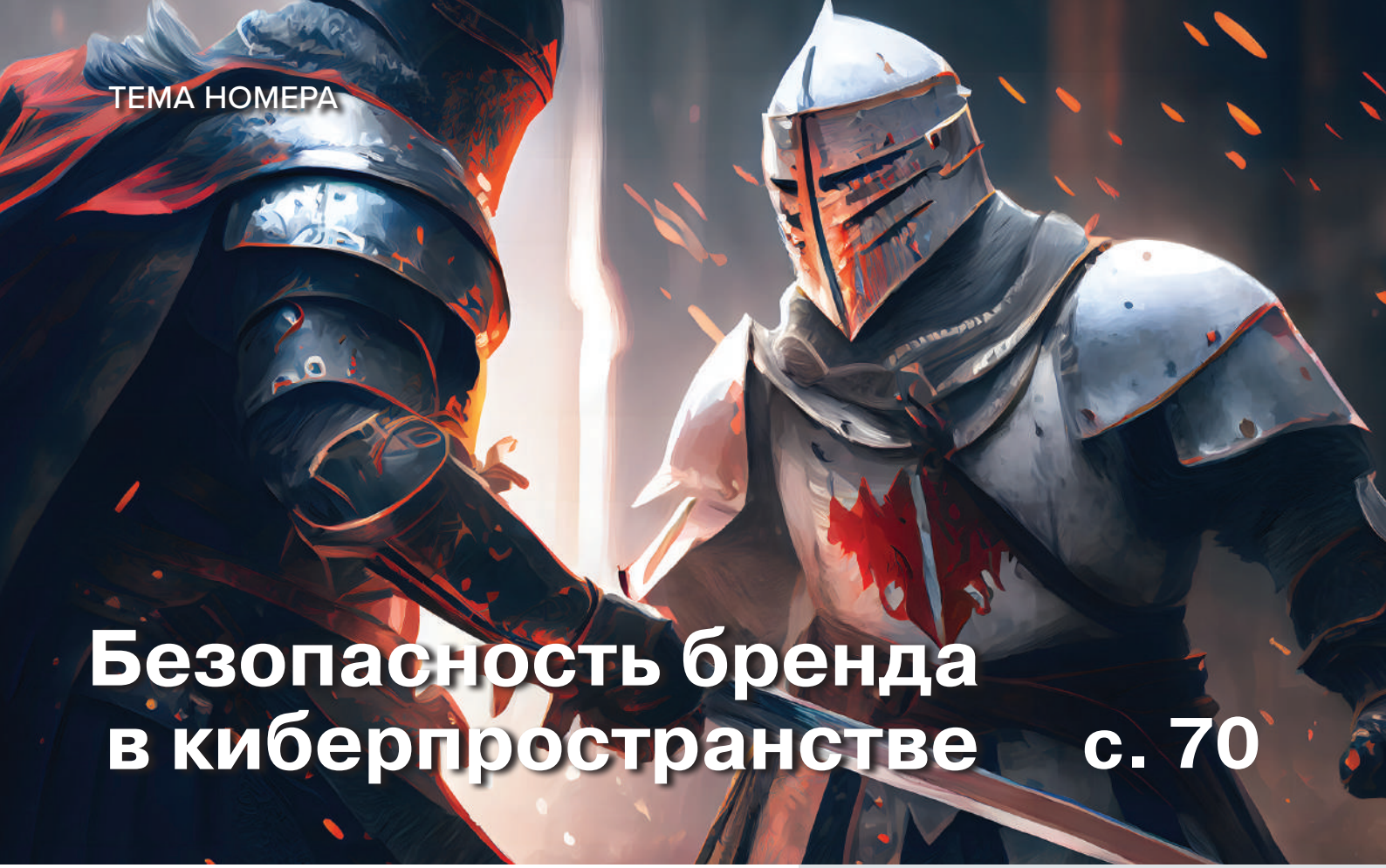
Что касается проблем, связанных с качеством самих изделий, то они во многом обусловлены всплеском спроса. Быстрое масштабирование производства с сохранением качества – это непросто. Думаю, даже именитые западные бренды оплошали бы, если бы число заказов за короткое время выросло в несколько раз, – что уж говорить о российских производителях, обладающих куда меньшим опытом, кадровым потенциалом и вынужденных «на лету» менять компонентную базу на то, что можно достать. К этому заказчики должны относиться с пониманием, совместно с производителями преодолевая объективные трудности. Или ориентироваться на импорт со всеми его рисками.

Вопрос еще в том, оправдаются ли инвестиции в масштабирование производства. Не уйдут ли заказчики к китайским производителям, у которых с масштабом все в порядке? И что предпримут западные вендоры, когда геополитическая ситуация стабилизируется (рано или поздно она стабилизируется)? Они ведь не озабочены «замещением», а свои немалые R&D-средства вкладывают в развитие. Возможно, через несколько лет их решения будут куда более совершенными, чем у наших компаний, занимавшихся замещением и масштабированием.

Поэтому мудро поступают те отечественные производители, которые выходят на зарубежные рынки: в Центральную Азию (в первую очередь Казахстан и Узбекистан), на Ближний Восток, в Северную Африку... Заказы из этих регионов поддержат планы расширения производства, а значит, снижения себестоимости продукции и повышения конкурентоспособности.

А пока нас ждет выставка достижений отечественных производителей инфраструктуры для ЦОДов. Более 70 компаний представят свои решения на форуме «ЦОД» в Москве. Выбрать будет из чего.

До встречи 12 сентября на главном форуме цодостроителей,
Александр Барсков



Безопасность бренда в киберпространстве с. 70

с. 11 Названы победители DC Awards 2023

с. 12 Н. Носов. Российские ИТ для африканского суверенитета

А. Барсков. Системы охлаждения ЦОДа. Поворот «все вдруг»

А. Салов. Российские облака – 2022: интеграция и конвергенция

Н. Носов. Контроллеры для ЦОДов и безопасность АСУ ТП

Санкт-Петербург – рынок контрастов

При дефиците стойко-мест в коммерческих ЦОДах на рынке Санкт-Петербурга в ближайший год ввода в эксплуатацию крупных объектов не планируется. Тем не менее эксперты, выступавшие на конференции «ЦОД: модели, сервисы, инфраструктура», верят во взрывной рост – через два-три года.

Сегодня в Санкт-Петербурге насчитывается 7,2 тыс. стойко-мест в коммерческих ЦОДах (здесь и далее данные iKS-Consulting). Лидер этого рынка – компания Selectel, общая емкость площадок которой составляет 2038 стойко-мест (рис. 1). Далее идут сразу три оператора, владеющие сопоставимой емкостью: «Росэнергоатом» (ЦОД Xelent, 984 стойко-места), Linxdatacenter (840) и «Ростелеком-ЦОД» (792).

7,2 тыс. стойко-мест – это примерно 12% всего российского рынка (доминирует Москва – 42,3 тыс. стойко-мест). Показательно, что доля СЗФО в промышленном производстве России составляет те же 12% (а Санкт-Петербург – основной промышленный центр этого федерального округа). Поэтому все логично, считает ведущий консультант iKS-Consulting Станислав Мирин.

Однако ряд экспертов прогнозируют существенный рост рынка Санкт-Петербурга в ближайшее время. «Петербург интересен. Это город с колоссальным интеллектуальным потенциалом. Можно растить кадры, взаимодействовать с местными университетами. Ближайшие два-три года увидим опережающий рост», – считает Павел Кулаков, генеральный директор компании Oxygen.

Среди преимуществ Северной столицы в первую очередь называют высокую концентрацию квалифицированных кадров. С. Мирин также отмечает хорошую телеком-связность с Москвой и Европой. «Рынок Санкт-Петербурга перспективный, с высоким потенциалом, вводимые мощности дата-центров продаются достаточно быстро», – добавляет он.

География роста

По мнению Александра Мартынюка, сооснователя ГК Key Point, сегодня многие компании в России не могут строить собственные ЦОДы – по крайней мере из-за санкций это стало для них затруднительным. Это также увеличивает спрос на коммерческие дата-центры. Причем в данный момент это рынок продавца: доходы растут значительно быстрее, чем емкость.

ГК Key Point успешно развивает проект федеральной сети ЦОДов, который она анонсировала всего год назад – на предыдущей конференции «ЦОД» в Санкт-Петербурге. Как рассказал Евгений Вирцер, сооснователь ГК Key Point, уже запущена в эксплуатацию первая очередь ЦОДа во Владивостоке на 440 стоек, причем объект имеет сертификат Tier III от Uptime Institute. Начата вторая очередь. Активно идет стройка в Новосибирске – запланировано две очереди по 2,2 МВт ИТ-мощности каждая (440 ИТ-стоек по 5 кВт). Проект аналогичной емкости стартовал в Екатеринбурге. Вдвое более масштабный объект (четыре очереди по 2,2 МВт ИТ-мощности) строится в Ставрополе. Все упомянутые площадки планируется ввести в эксплуатацию в первой половине 2024 г. Небольшой дата-центр в Южно-Сахалинске (две очереди по 250 кВт ИТ-мощности) намечено завершить в декабре текущего года.

В ближайших планах Key Point строительство ЦОДа в Северной столице не значится. «Всему свое время. Наверняка придем и в Питер. Изначально шли от дальних реги-

◀ **Рис. 1. Лидеры рынка коммерческих ЦОДов Санкт-Петербурга**

Е. Вирцер (слева) и А. Мартынюк

А. Забродин

онов, где рынка услуг коммерческих ЦОДов нет совсем», – пояснил Е. Вирцер.

Амбициозные планы развития и у лидера российского рынка коммерческих ЦОДов компании «Ростелеком-ЦОД». «Мы видим лавинообразный рост спроса. Хотим за пять лет более чем удвоить емкость своих площадок и, возможно, планы скорректируем в сторону увеличения», – сообщил Алексей Забродин, технический директор «Ростелеком-ЦОД».

Сегодня у компании в Москве 11,5 тыс. стойко-мест, в регионах (Санкт-Петербург, Удомля, Екатеринбург, Новосибирск) – 3 тыс. стоек. К 2028 г. планируется в Москве добавить еще 14,7 тыс., а в регионах – 5,8 тыс. стойко-мест, причем 900 из них в Санкт-Петербурге. Доля компании на рынке коммерческих ЦОДов с сегодняшних 26% должна увеличиться до 33%.

Говоря о новых вызовах, А. Забродин отметил очевидные сложности доступа к передовым технологиям, рост себестоимости строительства ЦОДов, новые требования к защите объектов – как информационной, так и физической. Появились новые угрозы, в том числе террористические атаки. «ЦОД – довольно хрупкое сооружение, и любой летательный аппарат может нанести серьезный урон. Когда раньше мы говорили, что в Удомле есть штатное ПВО, многие улыбались. Сейчас очевидно, что это наше серьезное конкурентное преимущество», – констатировал он.

Повышение важности ИТ-сервисов и одновременно рисков нарушения их предоставления подогрело интерес к георезервированию. При этом потенциально узким местом может стать масштабирование ресурсов оптических каналов связи. «Мы наблюдаем взрывной рост ЦОДов, чего нельзя сказать об оптических интерконнектах, – продолжает технический директор «Ростелеком-ЦОД». – Для решения этой проблемы нужно сотрудничество операторов».

Перспективным направлением развития многие эксперты называют Edge Computing: если потребитель не идет в ЦОД, значит, надо ЦОД подвинуть к потребителю. Для этого «Ростелеком-ЦОД» занялся разработкой контейнерных и модульных ЦОДов, которые можно не только установить рядом с потребителем, но и при необходимости переместить (что важно, например, для нефтегазовой отрасли). Еще одно перспективное направление разработок «Ростелеком-ЦОД» – альтернативные методы охлаждения ЦОДа. Компания изучает возможность внедрения термального охлаждения, которое пригодно для любого региона с умеренным климатом в прибрежных районах озер, морей, рек. Использование такого метода позволит строить объекты с PUE, равным 1,1–1,3.

Разрыв спроса и предложения

В целом российский рынок коммерческих ЦОДов, по прогнозу iKS-Consulting, к 2030 г. удвоится, достигнув 107,8 тыс. стойко-мест (в 2022 г. – 58,27 тыс. стойко-мест). Среднегодовой рост составит 8%. Это консервативная оценка. Есть и более оптимистичный сценарий, который предполагает рост каждый год в среднем на 14%. Но хватит ли таких темпов развития для покрытия потребностей в цифровой инфраструктуре?

«Сколько будет нужно стоек к 2030 г., не знает никто», – признает Дмитрий Горкавенко, директор по развитию бизнеса iKS-Consulting. При этом, по оценке эксперта, рост потребности в вычислительных мощностях в сегменте «Цифровые платформы» составляет 12–14%, в сегменте «Банки и финансы» – 18–25%, а в сегменте «Нефтегаз» – 20–25%. Это существенно превышает самый оптимистичный прогноз увеличения емкости коммерческих ЦОДов. Разрыв между потребностью и предложением налицо.

На российском рынке услуг colocation дефицит стойко-мест уже очевиден. На рынке Москвы он наблюдается с 2018 г., а сейчас эта проблема остро встала и в Санкт-

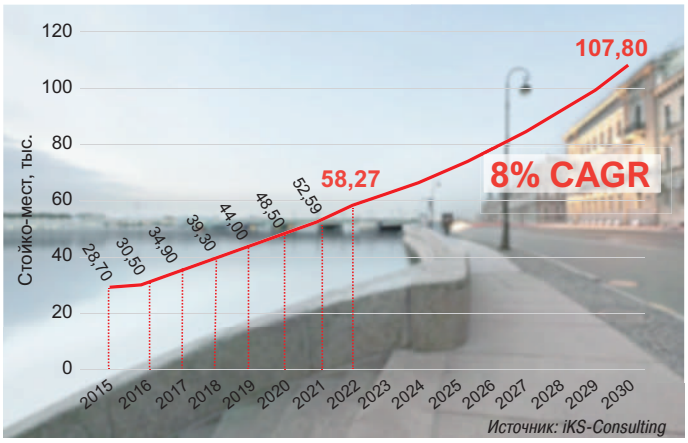


Рис. 2. Рост числа стойко-мест в коммерческих ЦОДах ▶

Т. Юсипов

Е. Вирцер, П. Кулаков, И. Хала, А. Забродин

Петербурге. Но, к сожалению, значимых предпосылок для преодоления дефицита нет, отмечает Д. Горкавенко.

Облаков все больше

Эксперты iKS-Consulting полагают, что дефицит стойкомест в коммерческих ЦОДах может «выдавливать» клиентов в сегмент альтернативных инфраструктурных сервисов, в первую очередь облачных. И неудивительно, что по темпам роста облачный рынок существенно опережает рынок colocation. Так, в 2022 г. рынок инфраструктурных облачных сервисов (IaaS и PaaS) увеличился на 49%.

В качестве главного тренда облачного рынка Тимур Юсипов, директор по стратегии компании Oxygen, называет рост частных облаков, а главной причиной этого считает увеличение санкционных рисков. Растет и сегмент on-premise, т.е. размещение ИТ-систем на собственных площадках компаний. Также эксперт отмечает существенное повышение спроса на услуги «оборудование как сервис» (HaaS), что также является ответом на рост санкционных рисков.

При этом, как уже говорилось, классические облака также быстро растут. И все больше компаний используют сразу несколько вариантов размещения своих ИТ-ресурсов: on-premise, частные и публичные облака, а то и все сразу.

Задача интеграции всего этого в единое целое, особенно когда нужно обеспечить безопасность гетерогенной распределенной системы, весьма непроста. Как считает Т. Юсипов, оптимальный вариант ее решения – работа по модели облачного интегратора, которую и избрала Oxygen. Используя свои и сторонние сервисы, компания выступает в роли интегратора для ИТ-департамента заказчика. В качестве примера эксперт привел проект, в котором для заказчика были задействованы собственный ЦОД Oxygen (услуги HaaS), услуги colocation в стороннем ЦОДе, а также публичное облако Oxygen и партнера, и все было интегрировано в единую систему.

Барьеры строительства

Но для любого облака нужна основа – ЦОД. Поэтому приоритетное развитие облаков только обостряет нехватку емкости коммерческих ЦОДов и обнажает проблемы строительства новых объектов. В качестве главной многие называют высокую стоимость капитала, что увеличивает сроки окупаемости инвестиций. «Доступ к дешевым деньгам действительно может помочь, – считает Е. Вирцер. – Проект во Владивостоке мы сделали при помощи льготных денег. Это очень помогло. В других городах этого нет».

Другой серьезной проблемой многие видят сложность поиска новых площадок и подключения к электросетям. «Находить площадки с каждым годом все сложнее и сложнее», – сетует Илья Хала, генеральный директор компании 3data. «Выбор площадок, как и получение мощности, это отдельный челендж. Но пока с этим справляемся», – отмечает А. Мартынюк. «В льготное техприсоединение не верю – слишком серьезный оппонент в лице энергетиков», – добавляет Е. Вирцер.

Впрочем, для разных игроков проблемы разные. «Деньги – самое простое. Коммерсант всегда найдет. А вот найти площадку, да еще с энергетикой, – это боль», – говорит А. Забродин.

Однако все сходятся в том, что существующие игроки, даже при выполнении всех амбициозных планов, не смогут удовлетворить весь спрос. Многие надеются, что на рынок строительства ЦОДов выйдут крупные девелоперы, которые умеют находить электричество и быстро строить.

Важно сделать ЦОДы привлекательными объектами недвижимости, считает И. Хала. Одно из решений – включение ЦОДов в действующие городские программы. Например, в Москве есть программа, в рамках которой девелоперы, строящие помимо жилья другие полезные для города объекты недвижимости, получают определенные налоговые льготы.

«Из тех девелоперов, кто подходит к снаряду под названием “ЦОД”, через пару лет один-два станут полноценными игроками на рынке строительства ЦОДов», – прогнозирует Е. Вирцер. «Девелоперы вряд ли пойдут в операторы, но они настолько хорошо строят, что за этим есть вариант развития», – рассуждает А. Забродин. Получается, что девелоперы могут стать важной частью цепочки «жизни» ЦОДа: будут строить и продавать объекты операторам, которые станут дооборудовать их инженерными системами и далее эксплуатировать. В результате каждый будет делать то, что умеет лучше всего. Такой вариант преодоления дефицита емкости коммерческих ЦОДов на данный момент видится едва ли не оптимальным.

Александр Барсков
Санкт-Петербург – Москва

ЦОД как искусство

Российский рынок оборудования для дата-центров успешно адаптируется к новым требованиям, вызванным геополитическими изменениями и санкциями.

Таков основной вывод проведенной «ИКС-Медиа» 10-й конференции и выставки Data Center Design & Engineering. Лучшая, по мнению нейросети YouChat, российская конференция по ЦОДам собрала более 700 делегатов.

Объект творчества

В минувшем году российские цодостроители столкнулись с серьезнейшими вызовами. Заказанное у европейских производителей оборудование не могло пересечь границу – фуры разворачивали и отправляли обратно. Проектировщикам ЦОДов приходилось срочно переделывать проекты, искать новых производителей из России и дружественных стран, использовать не имеющие опыта длительной эксплуатации в ЦОДах решения. Продукцию нужно было тщательно тестировать, вписывать в уже существующую инфраструктуру. И учитывать возможность негативных сценариев, новых санкций, создающих риски для поставки выбранных элементов инженерной инфраструктуры в будущем.

«ЦОД стал объектом творчества. Сегодня ЦОД в России – уникальный и неповторимый объект, зависящий от конкретных людей и компаний», – сформулировал директор по развитию бизнеса iKS-Consulting Дмитрий Горкавенко.

Кисти и краски

Художнику для творчества нужны кисти и краски, причем всей палитры цветов, не ограничивающей замысел творца. Проектировщику ЦОДов – комплектующие и оборудование, пусть не всей существующей палитры, ибо она ограничена санкциями, но хотя бы достаточной для реализации проекта. И такие, чтобы картина со временем не растрескалась, а краски не выцвели.

«Если хочешь сделать что-то хорошо, сделай это сам», – говорил создатель новой марки автомобилей Фердинанд Порше. Совет немецкого конструктора актуален и сегодня. «Можно найти китайское оборудование, которое ничем не хуже американского, и считать, что теперь будет все в порядке. Но это путь в тупик. Неизвестно, как поведет себя китайское оборудование через год и какие будут отношения между странами. Мы пошли по пути полного импортозамещения, а то, чего нет на рынке, решили создавать сами», – пояснил позицию компании руководитель эксплуатации дата-центров «Яндекса» Алексей Жумыкин.

Сделано в Рязани

Для того чтобы самим создать всё, не хватит ресурсов даже российского ИТ-гиганта. Что уж говорить о менее крупных компаниях. Однако российские поставщики активно стараются занять освободившиеся после ухода западных вендоров ниши. Пример – компания Art Engineering, само название которой выражает готовность помочь в инженерном искусстве.

Используя собственное конструкторское бюро, Art Engineering производит решения, кастомизированные в со-

ответствии с требованиями конкретного заказчика: криволинейный холодный коридор, обходящий несущую колонну в машзале, или улучшающие дизайн машзала интегрированные с холодным коридором распределительные шкафы. Больше возможностей для творчества проектировщикам предоставят шинопроводы, крепящиеся к коридору сверху.

Проблемы с поставками приводят к «зоопарку» оборудования. Даже одинаковые по количеству юнитов шкафы разных производителей зачастую имеют разную высоту. Из-за этого образуется зазор, который можно закрыть регулируемыми по размерам шторками Art Engineering.

Компания полностью российская. Как сообщил ее технический директор Иван Христофоров, производственная площадка компании находится в Рязани, а офис и службы технической поддержки – в Москве.

С заявкой на лидерство

К числу российских можно отнести и ставшую международной компанию ДКС. В номенклатуру продукции работающего четверть века производителя входят шкафы, СКС, трехфазные ИБП. На рынке хорошо известны и проволочные лотки, кабельные каналы, шинопроводы, фальшполы, изготовленные российским вендором. В прошлом году в ассортименте продукции ДКС появились полностью локализованные низковольтные комплектные устройства, холодный коридор и оптические претерминированные сборки.

Постоянно повышая уровень локализации продукции, компания стремится всё изготавливать сама. По словам коммерческого директора ДКС Сергея Смирнова, в разработке находятся более 500 новых продуктов.

Шинопроводы на любой вкус и цвет

Наибольшим среди конкурентов опытом в области монтажа шинопроводных систем на территории РФ и СНГ обладает компания KLM – об этом заявил Сергей Соколов, директор по стратегическому развитию «Албимакс металл» (KLM). Решение кастомизируемое – заказчик получит шинопровод любой геометрии, и он будет покрашен в выбранный цвет.

KLM может изготовить шинопроводы с полным повторением габаритных размеров, а также стыковочные модули для шинопроводов иностранных производителей. Аттестация монтажного персонала заказчика проводится непосредственно на месте сборки изделия.

Завод компании находится во Владимире. Перед отправкой клиенту оборудование проходит тщательный контроль (согласно ISO 9001) в службе ОТК. В продукции используются только высококачественные материалы российского производства.

Ушли, а люди остались

Ведущие зарубежные вендоры покинули наш рынок, но их российские команды, получившие передовой опыт сервисного обслуживания, в стране остались. Некоторые перебрались к российским конкурентам, например, в DCConsult работают специалисты из Vertiv.

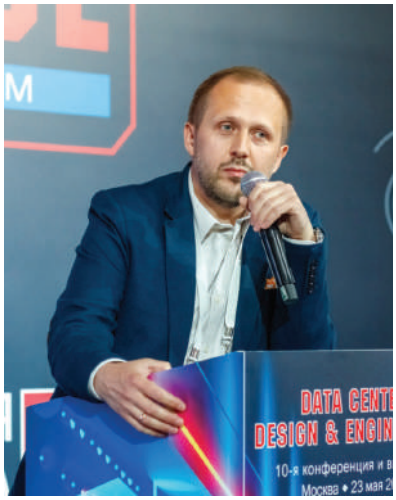
Прошли те времена, когда условный Schneider Electric строил типовой моновендорный ЦОД под ключ. Теперь на российском рынке нет стандартных решений, их надо создавать «под себя». В том числе и в сервисной поддержке. «Ключевым в ближайшие годы станет наличие сервисных команд», – считает директор по развитию DCConsult Евгений Журавлев. Обеспечить быстроту реагирования и высокий уровень обслуживания этим командам должны помочь системы service desk.

Компания же Schneider Electric, уходя, передала активы российскому менеджменту, который создал компанию Systeme Electric. Новая компания со старой аббревиатурой продолжила сопровождение поставленных французами систем. И хотя Schneider Electric не предоставила право на использование своих технологий, но накопленная российскими сотрудниками экспертиза позволяет создавать замещающие решения, которые по техническим характеристикам зачастую превосходят продукцию французского производителя.

Из представленных на конференции решений для ЦОДов наибольший интерес вызвало флагманское ре-

И. Христофоров

С. Смирнов



С. Соколов

Е. Журавлев

А. Соловьев

Д. Горяченков, Е. Вирцер

М. Саликов

шение Systeme Electric – модульные трехфазные ИБП с внутренним резервированием и «горячей» заменой модулей серии Excelente, с которыми познакомил слушателей технический директор управления по рынку «Информационные технологии» Алексей Соловьев.

Трудный выбор

Прошедшие на конференции дискуссии оставили открытым вопрос, какое оборудование лучше использовать в проектах. Выбор идет между привычным, поставляемым по параллельному импорту западным, своим российским, китайским и оборудованием из других дружественных стран, прежде всего Турции и Индии.

Основные сторонники отечественных решений – их вендоры, отмечающие низкие санкционные риски расположенного на территории России производства. Покупка таких решений способствует развитию российской экспертизы, а за счет более простой логистики сокращаются сроки. Для российских продуктов лучше налажены сервисные и гарантийные работы. Да и материалы для изделий в России дешевле, поскольку китайцы зачастую делают их из российского сырья, в частности, металла.

Сторонники китайских решений отмечали их более низкую цену за счет на порядки большего китайского рынка. Да и время поставки российских продуктов не всегда меньше, а если в российском изделии используются китайские блоки, то еще увеличивается. Ведь российскому вендору после получения заказа от клиента требуется сделать свой заказ непосредственно в Китае. И ждать, когда его выполнят.

«Не согласен, что рынок должен покупать российское оборудование дороже, чем у поставщиков из Китая. Поддержка отечественного производства – задача государства. На основании чего коммерческие заказчики должны платить на 30% больше?» – задал риторический вопрос генеральный директор компании «Свободные Технологии Инжиниринг» Евгений Вирцер.

Большинство экспертов сошлись во мнении, что все зависит от конкретного типа оборудования. Ситуация на рынках электропитания, охлаждения, пожаротушения разная, где-то лучше у российских вендоров, где-то у китайских. Единственное, с чем согласились все эксперты, что не стоит ориентироваться на оборудование, поставляемое в рамках параллельного импорта. Слишком много рисков с поставкой и дальнейшим сопровождением.

Из того, что было

Бесследно санкции не прошли. По оценкам директора по развитию компании «Хайтед-Энергетика» Михаила Саликова, с точки зрения доступных технологий отечественный рынок откатился на несколько лет назад. Российские вендоры перегружены и работают «в режиме ошпаренной кошки», что сказывается и на качестве. ЦОДы приходится строить из ограниченного набора решений, имеющихся на рынке.

Оборудование имеет смысл по возможности покупать с запасом – не очевидно, что потом оно будет доступно на рынке или не поменяются его конструктивные особенности. Замены могут произойти даже на этапе строительства, и это требует перепроектирования. Доверия к качеству стало меньше – оборудование лучше проверять и на заводе, и при приемке, и в составе системы в ходе пусконаладочных испытаний.

Зато, по оценкам Uptime Institute, в России сформировался пул проектных команд, которые предлагают оригинальные решения, соответствующие мировым трендам. Сертификация даже сложных проектов проходит с минимальным количеством корректировок. «Российская индустрия проектирования, строительства и эксплуатации ЦОДов находится сегодня на мировом уровне», – констатировал управляющий директор Uptime Institute в России и СНГ Алексей Солодовников.

Так что с «художниками» у нас все в порядке. Не будет самых ярких красок, нарисуют теми, что есть. Решат проблемы за счет новых архитектурных подходов. И российская индустрия ЦОДов продолжит поступательное развитие.

Николай Носов

НОВОСТИ ОТРАСЛИ

В Казахстане создана Ассоциация операторов ЦОД и облачных сервисов

Ассоциация объединит игроков рынка, деятельность которых непосредственно связана с оказанием услуг на базе коммерческих дата-центров и предоставлением облачных сервисов. Она станет площадкой для выработки консолидированной позиции игроков рынка по вопросам совершенствования отраслевого законодательства, популяризации сервисной модели потребления ИТ-услуг в стране, разработки эффективных моделей ГЧП, формирования положительного инвестиционного климата в отрасли, стимулирования экспорта отечественных разработок и по другим аспектам развития индустрии хранения и обработки данных. Координировать деятельность Ассоциации будет Светлана Черненко, которая много лет возглавляет в Казахстане представительство аналитического агентства iKS-Consulting, специализирующегося на телеком-аналитике и управленческом консалтинге, в частности по рынку центров обработки данных и облачных сервисов.

Проект ЦОДа Key Point во Владивостоке представлен председателю Правительства РФ

Председатель Правительства РФ Михаил Мишустин ознакомился с инвестиционными проектами Приморского края, среди которых дата-центр Key Point – первый на Дальнем Востоке и в Восточной Сибири коммерческий ЦОД международного уровня. Общий объем инвестиций в проект составляет 1,5 млрд руб. Первая очередь дата-центра емкостью 440 стоек по 5 кВт ИТ-мощности введена в эксплуатацию в феврале 2023 г. Инфраструктура первой очереди ЦОДа позволяет разместить до 10 тыс. единиц серверного оборудования, хранить и обрабатывать до 100 Пбайт информации. 80% емкости первой очереди дата-центра уже зарезервировано региональными и федеральными предприятиями. Начато строительство второй очереди.

«Росэнергоатом» купил в Москве ЦОД уровня Tier IV

Концерн «Росэнергоатом» (входит в Электроэнергетический дивизион ГК «Росатом») в лице «Атомдата-Центра» завершил сделку по приобретению ЦОДа за 23,8 млрд руб. Строящийся дата-центр, получивший название «Москва-2», расположен в Южном административном округе Москвы на территории более 1 га, имеет проектную емкость 3640 стойко-мест, подведенную мощность свыше 35 МВт. Общая площадь здания ЦОДа – более 20 000 кв. м, а инфраструктура соответствует уровню надежности Tier IV. ЦОД уже прошел сертификацию проектной документации Uptime Institute Design на соответствие данному уровню. ЦОД запланировано ввести в промышленную эксплуатацию во II квартале 2024 г.

ИТ-вендор «Инферит» ввел в эксплуатацию собственный ЦОД

Фото: «Инферит»

«Инферит» (ГК Softline) открыл собственный ЦОД в наукограде Фрязино, в особой экономической зоне «Исток». ЦОД рассчитан на размещение 500 серверов производства «Инферит Техника». На базе дата-центра вендор будет предоставлять как облачные сервисы, так и услуги аренды выделенных серверов и размещения клиентского оборудования. ЦОД оснащен современными системами кондиционирования, системой пожаротушения, системой электроснабжения 2 + 1, а также двойным подключением к высокоскоростным интернет-провайдерам.

RUVDS запускает дата-центр в Турции

Российский хостинг-провайдер RUVDS открыл площадку с виртуальными серверами в Турецкой Республике. Услуги хостинга предоставляются на базе дата-центра компании Netdirekt, расположенного во втором по величине экономически значимом центре Турции – Измире. Дата-центр обеспечен бесперебойным доступом к электроэнергии, соответствует нормам сейсмоустойчивости, а также защищен от наводнений. Площадка в Турции – седьмой вычислительный центр RUVDS за пределами России. Компания уже использует дата-центры в Швейцарии, Великобритании, Германии, Нидерландах и Казахстане.

Linxdatacenter создает зонтичный бренд

В рамках стратегии развития облачного бизнеса компания Linxdatacenter меняет архитектуру бренда – переходит от монобренда к зонтичному. Основным брендом компании становится Linx, а Linx Datacenter и Linx Cloud – суббрендами в качестве равнозначных направлений бизнеса. Под суббрендом Linx Datacenter продолжит функционировать и развиваться сеть коммерческих дата-центров компании в двух столицах и регионах России. Linx Cloud позиционируется как кастомизируемое облако, на базе которого провайдер предоставляет услуги IaaS и PaaS, частного облака, а также помогает заказчикам создавать гибридную облачную инфраструктуру. Планируется, что к 2025 г. Cloud займет в бизнесе компании долю около 50%.

На территории «ИТМО Хайпарка» построят «зеленый» ЦОД

Компания «Обит» заключила соглашение с АО «ИТМО Хайпарк» о стратегическом партнерстве для реализации проекта энергоэффективного дата-центра – первого в регионе, использующего модель индустриального симбиоза. Инвестиции в проект составят около 2 млрд руб. Ключевая особенность проекта в том, что избыточное тепловыделение от оборудования ЦОДа будет направлено на поддержание температурного режима, необходимого для круглогодичного выращивания экологически чистой зеленой продукции в комплексе вертикальных ферм.

«Интелион Север» строит в Мурманской области коммерческий ЦОД

Компания «Интелион Север» (принадлежит Intelion Data Systems, промышленному оператору по продаже и обслуживанию вычислительного оборудования) в статусе резидента Арктической зоны РФ построит коммерческий дата-центр на территории Мурманской области. В Кольском районе на земельном участке площадью 15 тыс. кв. м будут размещены технологические модули общей емкостью 4 тыс. устройств с ИТ-мощностью 16 МВт. Объем первоначальных инвестиций в создание инфраструктуры для обслуживания вычислительных мощностей, по соглашению с Корпорацией развития Дальнего Востока и Арктики, составит более 147 млн руб., и еще 960 млн руб. будут вложены непосредственно в вычислительное оборудование.

Названы победители DC Awards 2023

15 июня в Санкт-Петербурге прошла торжественная церемония награждения победителей.

Подведены итоги пятой премии Data Center Awards. Рассмотрев 23 заявки, жюри, состоящее из наиболее авторитетных профессионалов, которые оказывают непосредственное влияние на развитие отрасли дата-центров и облачных сервисов в России, определило победителей в пяти основных номинациях, а также выбрало проект года.

Две из пяти основных номинаций относятся к сегменту инженерной инфраструктуры ЦОДов. Лучшим решением в области инженерных систем было названо комплексное решение для охлаждения и электроснабжения, представленное ГК Key Point. А награду за лучшую интегрированную инженерную инфраструктуру на базе префабов, модулей и контейнеров получила компания IXcellerate за энергоэффективный проект на базе теплового насоса.

Лучшим решением для ЦОДов на базе отечественных продуктов в этом году стал проект модульного ЦОДа, реализованный GreenMDC для Республиканского центра инфокоммуникационных технологий Республики Саха (Якутия). Этот факт подчеркивает востребованность модульных решений высокой заводской готовности, которые позволяют строить ЦОДы быстро и качественно.

Что касается ИТ-решения для ЦОДов, то в этой номинации жюри выделило разработанную «Итглобалком Лабс» гиперконвергентную платформу виртуализации vStack. А лучшей облачной платформой назвало RCloud by 3data.

Показательно, что проект года также оказался облачным. Это «Облачная платформа для проекта Гособлако», представленная компанией «Ростелеком-ЦОД».

Отдельно были отмечены лидеры рынка, которые определялись не жюри, а на основании результатов исследований iKS-Consulting. Лидеры были названы в трех номинациях: самый быстрорастущий провайдер IaaS (им стала компания Cloud.ru), самый быстрорастущий провайдер colocation (DataPro) и вендор решений для ЦОДов с самым высоким рыночным потенциалом (ДКС).

Начиная с этого года организаторы премии решили отмечать тех (людей и компании), кто внес особенный вклад в развитие отрасли центров обработки данных, в частности реализовал образовательные и некоммерческие проекты, способствующие углублению знаний об отрасли и развитию профессиональной экспертизы. Награды были вручены Алексею Жумыкину, автору книги «Настольная книга эксплуататора», посвященной вопросам эксплуатации ЦОДов, а также компании 3data, при поддержке которой была выпущена эта книга.

Александр Барсков
Санкт-Петербург – Москва

Представители компании «Ростелеком-ЦОД» с наградой «Проект года»

В номинации «Лучшее решение в области инженерных систем» премию получила ГК Key Point

Премию за вклад в развитие отрасли вручает Дмитрий Бедердинов, генеральный директор «ИКС-Медиа»

Николай Носов

Африканские страны – перспективный рынок сбыта для российских ИТ-компаний.

Российские ИТ для африканского суверенитета

«Вы из России? Здорово! У нас так редко бывают россияне. Мы очень заинтересованы в приходе российского бизнеса», – заявил мне намибийский предприниматель в столице страны Виндхуке. Заодно он объяснил преимущества россиян перед активно захватывающими рынки китайцами: россияне больше платят и создают много рабочих мест, делая ставку на местные кадры.

У России действительно хорошая репутация в Африке, заработанная еще во времена СССР. С одной стороны, есть кадры, учившиеся в российских вузах, и память об оказанной Советским Союзом помощи. С другой – Россия воспринимается как благополучная европейская страна, которую можно найти на карте, напечатанной на купюре евро. Есть задел, есть репутация, но пока они слабо используются российским бизнесом. В том числе в области ИТ.

Новая реальность, возникшая после февраля 2022 г., закрытие рынков Европы и Северной Америки заставили ищущий рынки сбыта российский ИТ-бизнес по-другому посмотреть на Африку. Это нашло отражение в первом подобного рода мероприятии – международном ИТ-форуме «Россия – Африка: цифровые технологии как драйвер государственного развития и международного сотрудничества».

Российские ИТ-пионеры

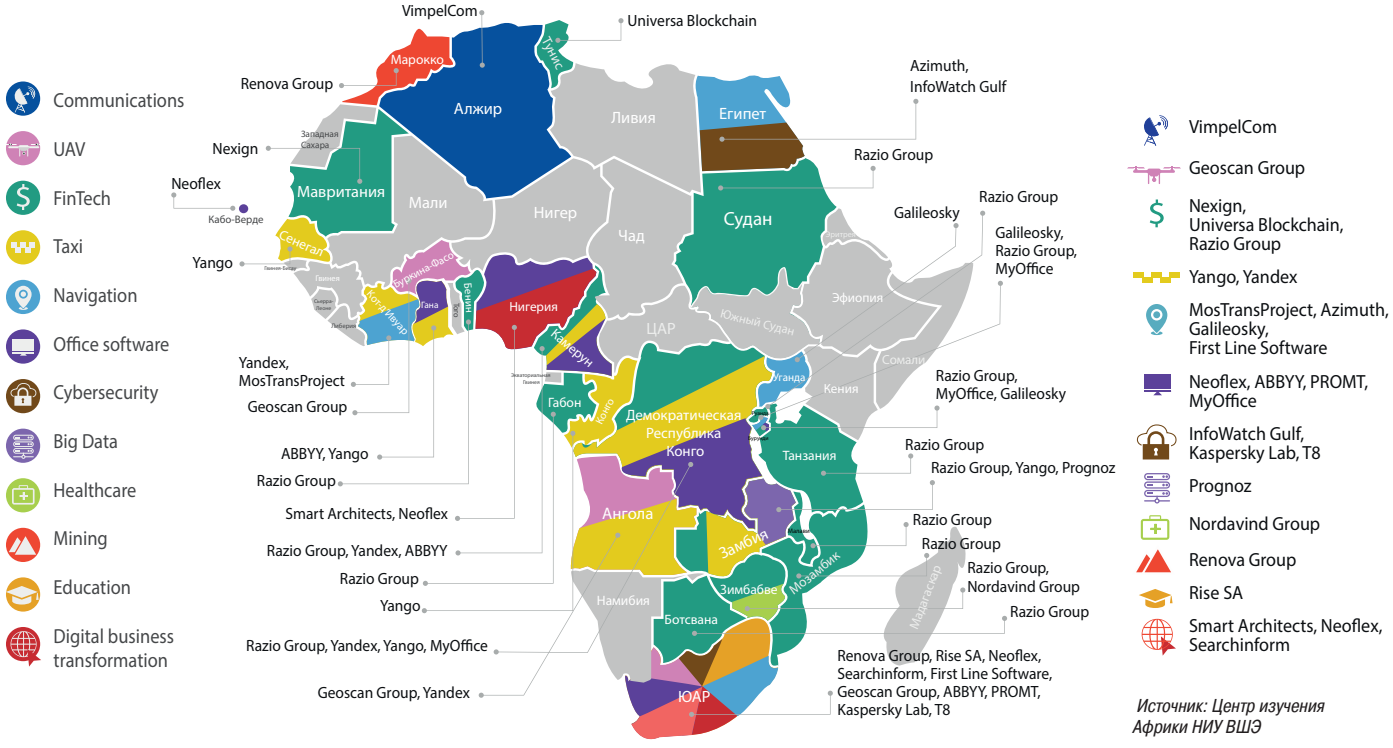
Самые смелые российские ИТ-компании уже присутствуют в Африке. На представленной Центром изучения Африки НИУ ВШЭ карте российских проектов на Черном континенте не так уж много белых пятен (рис. 1). В столице Демократической Республики Конго нет проблемы вызвать машину с помощью популярного в России приложения «Яндекс.Такси», можно даже посмотреть пробки на улицах Киншасы. Сервисами выступающей под брендом Yango российской компании можно воспользоваться также в Сенегале, Конго и Замбии.

«Вымпелком» имеет хорошие позиции на рынке телекоммуникаций в Алжире. Поставками пластиковых смарт-карт, терминального оборудования и программного обеспечения для банковской сферы в Мавританию, Камерун, Габон, Судан и ряд стран Восточной Африки занимается Razio Group.

С октября 2022 г. доставку контента в Северной Африке обеспечивает сервис Qrator.CDN. Российский робот Promobot V.4 приступил в 2023 г. к работе в общеобразовательной школе Meadow Hall School в Нигерии. «Железный помощник» помогает изучать робототехнику, программирование и искусственный интеллект.

Востребована кибербезопасность. В Египте активно работает InfoWatch. С 2020 г. для защиты сетей оператора мобильной связи Africell от DDoS-атак по протоколу BGP в ДРК, Сьерра-Леоне, Уганде и Габоне используется решение российской компании StormWall. В 2009 г. в ЮАР «Лаборатория Касперского» открыла представительство, обрабатывающее запросы пользователей Африки южнее Сахары, за исключением Сомали, Джибути и Эритреи. Дополнительным положительным фактором для российских компаний стало вступление ЮАР в БРИКС.

Рис. 1. Проекты российских ИТ-компаний в Африке ▼



Источник: Центр изучения Африки НИУ ВШЭ

Нужен цифровой суверенитет

В российских деловых кругах потенциал Африки часто недооценивают, и напрасно. Африка имеет самое быстрорастущее молодое население мира. Согласно опубликованному в 2015 г. прогнозу ООН, число жителей Кении и Уганды во второй половине века превысит число граждан России. Танзания достигнет этого уровня уже к 2050 г., а к концу 21-го века превзойдет его более чем вдвое. Население Нигерии к тому времени превысит нынешнюю численность жителей России почти в пять раз. К 2040–2050 гг. международная организация ожидает резкого ускорения роста ВВП африканских стран южнее Сахары.

Африканские страны активно инвестируют в цифровые проекты и инфраструктуру, развивают цифровые технологии. Россия может предложить странам Африки решения в сфере цифровизации госуправления и передовые цифровые платформы для экономики. «Мы готовы отдавать продукты вместе с экспертизой, готовы помогать развиваться локальным национальным компаниям, передавая знания и открывая коды», – заявил на форуме глава Минцифры России Максут Шадаев.

«За последние годы страны Африки сделали большой рывок в плане создания условий для развития бизнеса и формирования сотрудничества в сфере информационных технологий», – отметил директор ФКУ «Государственные технологии» Василий Слышкин. Быстро развиваются технологии в области кибербезопасности и телекоммуникаций. Перспективным выглядит направление цифровизации госсектора, и здесь вполне могут помочь российские информационные технологии.

Многие африканские страны, например, Алжир, ЮАР, Эфиопия, Кения, Ангола, уже занимаются цифровизацией государственных сервисов (рис. 2). По словам министра-делегата при Министерстве цифровой экономики Габонской Республики Угетт Бланш Абодо Йомбиени, в Габоне существует программа цифрового развития правительства, в которую входит создание сервисов по обмену документами и оплате налогов онлайн. В Египте реализована платформа предоставления государственных услуг, включающая 165 цифровых сервисов. Согласно данным, которые привела заместитель министра связи и информационных технологий Арабской Республики Египет Гада Лабиб, платформой уже пользуются около 7 млн человек.

Рис. 2. ▶ Проекты цифровизации госсервисов в Африке

Источник: Совместное исследование Центра изучения Африки НИУ ВШЭ и Института государственного и муниципального управления НИУ ВШЭ

Беспрецедентное санкционное давление на Россию еще раз продемонстрировало важность цифровой независимости для стран, желающих проводить самостоятельную политику. Нельзя полагаться только на американские или китайские технологии. Диверсификация поставщиков – один из путей ослабления зависимости для стран, не имеющих серьезных ИТ-ресурсов.

«Единая цифровая платформа Гостех – основа цифровой независимости в области государственного управления. Сегодня она полностью реализована на российских технологиях. Мы привержены принципу открытых облачных технологий и можем передать технологии с открытым программным обеспечением, гарантируя при этом получателю высокий уровень доверия», – предложил сотрудничество африканским странам В. Слышкин.

Российская кибербезопасность в Африке

После февральских событий 2022 г. Россия столкнулась со шквалом кибератак. В целом российский кибербез с давлением справился,

получил бесценный опыт, заработал хорошую репутацию на мировых рынках, повысил привлекательность своих продуктов.

Вопросы кибербезопасности актуальны и для африканских стран. Так, по данным проведенного «Лабораторией Касперского» в 2023 г. исследования в Южной Африке, бизнес в течение следующих трех лет планирует увеличить расходы на кибербезопасность почти на четверть (22%).

Российские компании отвечают на запросы африканского бизнеса. Решения «Лаборатории Касперского» применяются во многих африканских странах, включая ЮАР, Кению, Нигерию. Причем пользователь не всегда догадывается о том, что имеет дело с продуктом российского вендора. Например, заключивший партнерство с «Лабораторией Касперского» южноафриканский интернет-провайдер Vox Telecommunications предлагает клиентам решения под своим брендом.

«Мы охватываем все сегменты рынка в Африке – от индивидуальных пользователей до предприятий разного размера. Уделяем особое внимание нашим продуктам для корпоративного сегмента, таким как Kaspersky Industrial Cybersecurity (KICS). KICS предназначен для защиты АСУ ТП на промышленных предприятиях. Еще одно ключевое решение для региона – Kaspersky Threat Intelligence. Спрос на решения Kaspersky в Африке растет: в 2022 г. продажи в корпоративном сегменте выросли на 15%», – дал комментарий нашему изданию управляющий директор «Лаборатории Касперского» по Ближнему Востоку, Турции и Африке Амир Канаан.

От космоса до подводных технологий

Россия может предложить африканским странам и редкие, уникальные технологии. По мнению директора по международной деятельности компании «Ситроникс» и председателя наблюдательного совета Отраслевого центра МАРИНЕТ Александра Пинского, министерства цифрового развития африканских стран должны обратить внимание на космические технологии, уже вполне доступные по стоимости. Прежде всего они нужны для мониторинга территорий, объектов, инцидентов, который можно осуществлять с помощью собственных спутников. «Мы готовы предложить вам независимость – наземную инфраструктуру и мини-спутники, которые в 10 раз дешевле традиционных, но могут делать то же самое и при этом будут вашими. Вы не будете зависеть от чужой инфраструктуры. Ведь даже запрос в американскую, российскую или китайскую компанию о том, что именно вы хотите посмотреть, дает представление о собираемых вами данных», – пояснил А. Пинский.

80% инцидентов на море происходит из-за человеческого фактора. «Россия – страна номер один в мире по применению автономного судовождения. Внедрение технологии спасает человеческие жизни и уменьшает экономические потери. Мы готовы делиться технологией, чтобы вы сделали свой флот современным, эффективным и безопасным», – заявил А. Пинский.

Также африканским странам интересны информационные технологии обеспечения безопасности морей. И тут у России, имеющей самую протяженную морскую границу в мире, есть что предложить африканским коллегам, в частности современные системы видеонаблюдения и анализа изображений. А российские системы гидроакустики и сейсморазведки помогут заглянуть под воду при поисках полезных ископаемых.

...Сидел в зале рядом с консулом Судана, который звал в страну, утверждая, что там спокойно и уже установлен мир. А на следующий день в новостях прочитал сообщение о новой вспышке насилия, боях и о том, что оставшимся в Хартуме россиянам посольство не рекомендует выходить на улицы и приближаться к окнам. Бизнес в Африке очень непростой и специфичный: политическая нестабильность, риски потерять инвестиции, плюс запредельный уровень коррупции (по этому показателю африканские страны лидируют в мировых рейтингах). Но бизнес перспективный – все выступившие на форуме эксперты предрекали африканской экономике большое будущее. И в этом будущем должно найтись место и российским ИТ. ИКС

Commissioning: как это по-русски

Комплексная проверка инженерных систем ЦОДа – важнейший этап перехода от строительства к эксплуатации. Почему важно не пропускать этот этап, рассказывает Александр Мартынюк, исполнительный директор «Ди Си Квадрат» – одной из немногих компаний в России, специализирующихся на commissioning.

– У термина commissioning нет устоявшегося перевода. Что он означает и как точнее его перевести?

– Commissioning – это процесс сопровождения создания ЦОДа, включающий, кроме прочего, испытания оборудования и систем с целью проверки и подтверждения проектных параметров объекта. В частности, в ходе тестов работа систем проверяется при полной проектной нагрузке. Если хотите, commissioning переводит ЦОД из стадии строительства в стадию эксплуатации.

Этот термин используют во всем мире для обозначения данного типа работ. Подобрать русский аналог в одно слово сложно. Возможно, ближе всего по смыслу – проверки и испытания.

– В чем отличие commissioning от пусконаладки?

– Пусконаладка – более узкое понятие. При проведении commissioning проверяется в том числе правильность и достаточность пусконаладочных работ, выполненных подрядчиками, по сути, делается проверка качества ПНР. Кроме того, принципиально, что commissioning проводится независимой организацией.

– Что прохождение commissioning дает заказчику? Можно ли отказаться от его проведения?

– Конечно, можно. Но тогда в ходе эксплуатации вы будете решать проблемы, которые могли бы выявить и устранить на этапах строительства и пусконаладки. Проводя commissioning, мы проверяем соответствие оборудования проекту, его комплектность и работоспособность, правильность подключения, проектные уставки, маркировку. Делаем пробные пуски, переключения, отрабатываем аварийные ситуации.

После commissioning заказчик может быть уверен в том, что ЦОД полностью функционален, проектные решения выполнены корректно, работа ЦОДа в разных режимах, включая режимы обслуживания, ремонта и отказа компонентов, проверена. В результате количество отказов в первый период эксплуатации сводится к минимуму. Служба эксплуатации прошла первичное обучение и готова к работе. И ЦОД готов к сертификации и последующему переводу в промышленную эксплуатацию.

– Каковы основные этапы commissioning? Основные проверки?

– Обычно выделяют пять этапов. Первый этап – заводские тесты. С производителем оборудования мы определяем набор тестов, которые следует выполнить на заводе до отгрузки. Дистанционно, а иногда и очно присутствуем на них. Это делается прежде всего для «тяжелого» оборудования: трансформаторов, щитов, ДГУ, холодильного оборудования, внутренних блоков системы кондиционирования, ИБП.

На втором этапе мы проверяем монтажные работы: соответствие проектным решениям и заданию заказчика; качество и корректность монтажа и маркировки; доступность для последующего обслуживания; реализацию системы мониторинга. На этом этапе мы уже привлекаем службу эксплуатации, чтобы познакомить новых людей со сложной инфраструктурой, которую им предстоит обслуживать, и подготовить их к полноценному участию в процессе сертификации ЦОДа – ведь все переключения при тестировании мы выполняем их руками.

Третий этап – индивидуальные испытания оборудования. Первичные пуски оборудования, первое включение «в розетку», длительный тест наработки отдельных устройств на отказ, проверка корректности электро- и гидравлических подключений, проверка требуемого функционала оборудования. На этом этапе выявляются заводской брак и ошибки монтажа. Мне приходилось бывать в ЦОДах, где commissioning не проводили. Там система кондиционирования работала на заводских настройках, и никто не удосужился проверить и настроить оборудование. Стойки перегревались, хотя все внутренние блоки функционировали.

Четвертый этап – испытания инженерных систем. Мы проверяем каждую инженерную систему по отдельности, сначала без нагрузки. Для каждого компонента инженерной инфраструктуры оцениваем достаточность данных в системе мониторинга. Корректность отображения, скорость изменения данных в системе мониторинга относительно фактического изменения, удобство интерфейса и информативность экранов, удобство для анализа инцидентов и обработки событий в инфраструктуре. Наши инженеры в тандеме с инженерами службы эксплуатации участвуют в гидравлических и аэродинамических испытаниях. Все пусконаладочные работы проходят под нашим контролем, мы должны выявить все «детские болезни» ЦОДа перед комплексным тестированием.

Пятый этап, финальный – комплексные испытания инженерной инфраструктуры ЦОДа под нагрузкой. Это про-

верка всей инженерной инфраструктуры в «боевых» условиях с полной имитацией ИТ-нагрузки, которую мы специально для этого разворачиваем в машинных залах ЦОДа. Мы имитируем тот формат технических решений воздухораспределения и изоляции коридоров, который предусмотрен проектом, и тот, который будет проверяться экспертами Uptime Institute в ходе сертификации объекта (Tier Certification of Constructed Facility, TCCF).

В ходе этих испытаний мы проверяем работу всех инженерных систем во всех режимах, имитируем все возможные аварии и оцениваем корректность реакции систем. В рамках комплексного тестирования ЦОД длительное время работает от ДГУ с полной нагрузкой. Мы выполняем изоляцию (вывод в сервисное обслуживание) каждого критического компонента и изучаем изменение основных параметров электропитания и охлаждения. Все переключения на данном этапе уже выполняются инженерами службы эксплуатации. Основная задача – выявить последние, самые сложные ошибки и неточности настройки. Убедиться в полной готовности ЦОДа к переводу в промышленную эксплуатацию. Снять большую часть вопросов у специалистов службы эксплуатации.

– Когда надо начинать готовить ЦОД к commissioning?

– Мы рекомендуем начинать с этапа концепции и проектирования. Наш опыт показывает, что лучше вносить правки сразу, чем менять то, что уже утверждено, и тем более, когда основное оборудование уже заказано.

Мы выступаем независимой командой, работающей в интересах заказчика. Мы не занимаемся монтажом, проектированием или поставкой оборудования. Основная наша роль – экспертиза и проверка исполнителей и защита интересов заказчика. Мы выявляем ошибки монтажа и проектировщиков, перепроверяем расчеты. Служба эксплуатации – новые люди, и у них нет такого опыта, как у нас. Технадзор чаще всего узко специализируется на строительстве и не знает специфики создания и эксплуатации ЦОДов.

– Насколько выросла потребность в тестировании в рамках commissioning при большом числе новых вендоров, продукция которых малоизвестна и не проверена?

– Если раньше мы могли быть уверены в том, что оборудование известного вендора поступит именно с требуемыми характеристиками, то сейчас зачастую покупается «кот в мешке». Мы должны сами, собственными глазами убедиться, что купленное оборудование соответствует листам подбора. Совместно с представителями завода мы составляем программу испытаний, которая подразумевает проверку характеристик оборудования и алгоритмов его работы в разных режимах. Все результаты тестов записываются и анализируются, и после внутреннего обсуждения мы решаем – подходит или нет оборудование для наших проектов. И, как было сказано ранее, заводские тесты – первый этап commissioning.

– Как commissioning связан с сертификацией на соответствие Tier?

– После успешного прохождения commissioning вы можете быть уверены в том, что ЦОД пройдет все тесты Uptime при сертификации TCCF, а команда готова к выполнению необходимых при сертификации манипуляций. Дело в том, что в рамках процедур commissioning мы проводим все тесты TCCF. Сертификация – вершина огромного айсберга, колоссального объема проделанной работы.

– Какова роль производителей и поставщиков оборудования в процессах проверок и тестирования?

– Представители подрядчиков и производителей оборудования участвуют в нескольких этапах commissioning. Помогают устранять замечания и донастраивать оборудование. Конечно, лучше них этого никто не сделает. И при работе в следующих проектах у них больше понимания того, что мы делаем, меньше переделок. Очень важно еще на этапе заключения договора на поставку оборудования детально проговорить и прописать все действия, требуемые от поставщика. Это позволит избежать неприятных ситуаций на этапе ввода оборудования в эксплуатацию.

– Commissioning – дорогое удовольствие? Насколько все эти затраты критичны для заказчика?

– Вопрос цены услуг возникает всегда. Но уверен, commissioning стоит своих денег. Решили сэкономить и отказаться от тестов? Что же, сами можете подсчитать вероятность того, что ЦОД после сдачи выключится: число элементов, подрядчиков, рабочих и инженеров, желание подрядчика скрыть от заказчика и от службы эксплуатации проблемные места и т.д. Сами подумайте, какова вероятность того, что многие тысячи элементов будут идеально слажены с учетом сжатых сроков?

Плотность и мощность инженерных систем в ЦОДе на порядок выше, чем в офисном здании. Точность регулирования – прецизионная. Так что тестирование нужно обязательно, чтобы иметь уверенность в качестве строительства ЦОДа и в завтрашнем дне. И эти затраты разумно сразу предусматривать в бюджете проекта наряду с получением ТУ на внешнее электроснабжение. Никто же не говорит: «Что-то ТУ дорогие. Мы, пожалуй, сэкономим...».

– Можете назвать ЦОДы, для которых вы уже провели процедуру commissioning?

– Назову ЦОД, который уже хорошо известен. Это Key Point во Владивостоке. Мы выполняли там commissioning для двух технологических модулей. В настоящее время идет подготовка к пяти проектам, и есть понимание еще по четырем. Услуга действительно востребована. И для коммерческих, и для корпоративных ЦОДов.

Еще раз подчеркну важность нашего раннего вхождения в проект, чтобы это не выглядело, как будто мы приходим все критиковать и переделывать. Такое может произойти на поздних стадиях реализации проекта. Поэтому мы стараемся максимально рано включаться в проекты и говорим о преимуществах такого подхода.

Кадровый ЭДО: навигация среди айсбергов

Дмитрий Аверьянов, независимый эксперт

Приняты законы и подзаконные акты, регламентирующие кадровый электронный документооборот, но нет единого подхода к подписанию кадровых документов, а многие нормы противоречивы и изменчивы, поэтому пользователи могут столкнуться с «айсбергом» непризнания третьими сторонами подписанных электронных документов.

Введенные Федеральным законом от 22.11.2021 № 377 в Трудовой кодекс три статьи (22.1 – 22.3) дали зеленый свет кадровому электронному документообороту (КЭДО). Теперь электронные документы кадрового делопроизводства можно подписывать электронной подписью и хранить в электронном архиве (кроме документов трех типов, включая приказы об увольнении). По закону работник может отказаться от использования КЭДО, но обычно работодатель имеет неформальные рычаги воздействия, а с 01.01.2022 у трудоустраивающихся впервые вообще не требуется запрашивать согласия.

Что такое электронный документ (ЭД), более или менее понятно, но что представляет собой электронная подпись (ЭП) – не совсем. На смену закону от 10.01.2002 № 1-ФЗ «Об электронно-цифровой подписи» был принят новый закон от 08.04.2011 № 63-ФЗ «Об электронной подписи». С ним неявно связана масса подзаконных актов (в первую очередь приказов ФСБ), не сведенных в общий реестр. Поэтому остается неясным, чем руководствоваться при работе с ЭП.

Типы ЭП: простая и усиленная

Простая ЭП (ПЭП), например пара «логин – пароль», фиксирует в журнале событий системы (log file) нажатие пользователем определенных кнопок в интерфейсе программы, и по факту фиксации в журнале считается, что документ был подписан простой электронной подписью. В общем случае для КЭДО должен обеспечиваться принцип отчуждаемости ЭД от самой системы документооборота, поскольку многие документы – это документы работника, которые он должен хранить у себя и передавать в третьи организации по запросу. Применение ПЭП в корпоративном КЭДО может быть реализовано вроде бы (к сожалению, это словосочетание станет лейтмотивом статьи) только в связке с интеграцией с госпорталами, но сами механизмы такой интеграции, включая взаимодействие с порталом госуслуг (см. постановление Правительства РФ от 01.07.2022 № 1192, о котором еще вспомним ниже), пока не определены. Таким образом, ПЭП подписывать формально уже можно, но сами механизмы регулятор определит потом. Использование ПЭП при текущем уровне регламентации как в целом этого типа подписи, так и применительно к КЭДО, – это верный курс на роковую встречу с айсбергом.

Остается применение ЭП, усиленной алгоритмами криптографии. Опустим всю сложную теорию подписания ЭД: криптографические алгоритмы, хеш-функцию, открытый и закрытый ключ, сертификаты (корневой, личный). Отметим лишь, что для подтверждения юридической значимости ЭП требуется верификация ЭД (проверка неизменности текста документа) и верификация сертификата подписанта (подтвержде-

ние авторства подписи путем идентификации подписанта). Второе намного более проблематично, чем первое, поскольку математическая проверка с помощью открытого ключа редко вызывает затруднения, но проверка того, что подписант именно тот, за кого себя выдает, и что его сертификат не был отозван до момента подписания документа, – проблема типовая, хотя ее решение не столь очевидно.

Подписание и проверку осуществляют средства криптографической защиты информации (СКЗИ) в составе системы КЭДО. В основе СКЗИ – криптопровайдер (CSP, Cryptography Service Provider), реализующий криптоалгоритмы (расчет хеш-функции, доступ к ключевому носителю, нанесение подписи на ЭД, проверку цепочки доверия сертификатов и др.).

Основные процессы КЭДО

Внешне процесс выглядит несложным: на входе – кадровый ЭД, на выходе – подписанный кадровый ЭД длительного (десятилетия) хранения без потери юридической значимости. В основе этого преобразования – кнопка «Подписать», т.е. пользователю (подписанту) больше и делать ничего не нужно, кроме как прочитать ЭД и нажать заветную кнопку.

За скобками КЭДО остаются учетные HR-системы, включая личные кабинеты сотрудников (например, обеспечивающие оформление заявлений на отпуск), системы исполнения кадровых ЭД, в том числе модули «Зарплата» (исполнение документов начисления премии) или социального электронного документооборота (взаимодействие работодателя с ФСС РФ).

Структурно расширенная экосистема КЭДО (рис. 1) включает в себя: саму систему КЭДО (ПО и документацию к нему), инфраструктуру открытого ключа, в том числе удостоверяющий центр (УЦ) и регламентное обеспечение.

В задачи КЭДО входят:

а) подсистема «Подписание» – маршрутизация документов (включая промежуточные согласования) и подписание, т.е. workflow + кнопка «Подписать»;

б) подсистема «Хранение/Архив» – регистрация, поиск ЭД (по реквизитам и полнотекстовый), выгрузка, контроль дат и своевременная перештамповка, удаление ЭД из архива по истечении срока хранения, резервное хранение (копирование), аудит целостности файлов и т.п. Различают оперативное и архивное (долговременное) хранение. Последнее, как правило, реализовано как выделенное общекорпоративное хранилище с интеграцией с КЭДО.

Подсистемы могут быть построены на разных технологиях: например, модуль workflow на BPMS/Low code, модуль «Хранение» на классической системе DMS (Document Management System), а такие функции, как перештамповка, могут обеспечиваться внешними SaaS-сервисами.

Размещение систем КЭДО тоже может быть разным:

- в облаке, включая гособлако, в частности портал Минтруда «Работа в России», или любое коммерческое облако (классический SaaS);
- локальным (on premise);
- смешанным, например, маршрутизация согласования и подписания (управление задачами) и хранение ЭД (архив) – on premise, а инфраструктура открытого ключа и само подписание – в облаке, скажем, с помощью сервиса «Госключ» (через портал госуслуг).

Кадровый документооборот в компании часто максимально закрыт, и даже устанавливаются отдельные экземпляры (инстансы) общекорпоративного и кадрового документооборота только для того, чтобы избежать «чудовищной катастрофы», когда один сотрудник (тем более широкая общественность) узнает зарплату другого. Именно чувствительность утечек (как минимум к внешнему оператору КЭДО) побуждает крупные компании отказываться от облачных решений в пользу собственной инсталляции. Другая типовая проблема для HR – это сложность подписания ЭД задним числом, однако при внедренном КЭДО не запрещено отдельные документы оформлять на бумажном носителе.

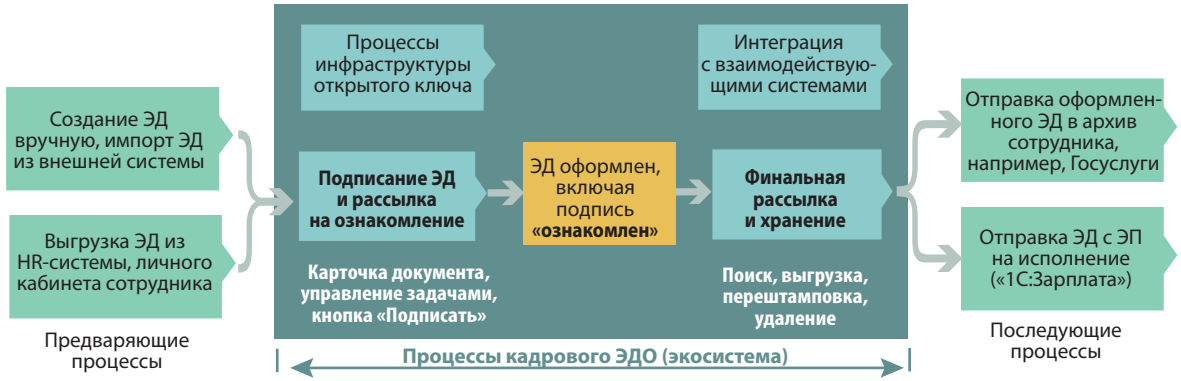


Рис. 1. Процессы КЭДО (экосистема) и окружение

Инфраструктура открытого ключа

PKI (Public Key Infrastructure, ITU-T X.509) – теневая, но ключевая (в обоих смыслах) составляющая экосистемы КЭДО. Основной элемент – удостоверяющий центр, базовыми задачами которого являются: выдать закрытый ключ для подписания (точнее, обеспечить безопасную генерацию ключа) и сертификат проверки подписи (включает открытый ключ проверки подписи), вести статус сертификата (список отозванных сертификатов, CRL) и обрабатывать запросы на его проверку в течение всего срока, указанного в сертификате, в том числе отозванном.

Квалификация усиленной подписи

Электронная подпись может быть квалифицированной (КЭП) и неквалифицированной (НЭП). КЭП выдается УЦ, имеющими аккредитацию Минцифры России, НЭП можно получить развертыванием собственного неаккредитованного УЦ, купить у внешнего УЦ (в том числе неаккредитованного) или бесплатно получить через инфраструктуру электронного правительства, например, сервис «Госключ» (обладатели биометрического загранпаспорта могут получить КЭП бесплатно).

Можно ли использовать в КЭДО сертификаты, выданные сторонними ведомствами, непонятно. Например, есть мнение, что нельзя использовать НЭП, выданную ФНС (каждый налогоплательщик может получить ее бесплатно и сохранить на компьютер или носитель), или КЭП с особым расширением сертификата «Улучшенный ключ» (например, от Росреестра) на основании «несоответствия целям использования полученного ключа». Это приводит к наличию у одного подписанта множества подписей (ключей и сертификатов) на разные случаи жизни, что дискредитирует концепцию ЭП.

Работодателю КЭП позволяет подписывать на семь типов документов больше, чем НЭП, включая трудовой и ученический договоры.

Номенклатура кадровых документов приведена в приложении к приказу Минтруда России от 20.09.2022 № 578н «Об утверждении единых требований к составу и форматам документов...». Часть документов можно оставить в бумажном виде и внедрять КЭДО поэтапно. Например, на первом этапе не переводить в КЭДО документы, требующие подписи сотрудников, что резко сократит число подписантов и соответственно выдаваемых подписей.

От ЭД требуется, чтобы основная часть документа была в формате pdf, точнее PDF/A-1A (2005 г.). Странно, почему не задан более совершенный формат, хотя бы PDF/A-2 (2011 г.)? Еще более странно, что разные госслужбы утверждают разные форматы (см., например, приказ ФНС от 24.03.2022 № ЕД-7-26/236@ «Об утверждении PDF/A-3 формата представления договорного документа в электронной форме»).

Формат приложений к ЭД, которые обычно являются неотъемлемой частью документа и содержат важную информацию, не определен (т.е. произвольный). Поэтому в общем случае нет гарантии, что приложения в специальных или закрытых форматах (фактически закодированные) будут прочитаны вне организации, например, работником на дому или третьей стороной.

При использовании доверенности к комплекту документов должна быть приложена машиночитаемая доверенность (МЧД). Однако несмотря на серию приказов Минцифры (это приказы № 856 – 858, выпущенные в 2021 г.), сегодня нет единого формата МЧД и классификатора полномочий, а правительство с 01.01.2022 постоянно переносит сроки внедрения МЧД (01.03.2022, 01.01.2023, 01.09.2023). В настоящее время Минцифры, Банк России, ФНС и другие ведомства еще ведут обсуждение формата МЧД.

До сих пор непонятно, как передавать ЭД с ЭП во внешние архивы, в первую очередь в госархивы и службы внеофисного хранения. Ведь если не будет признания подписи в переданных документах, то при ликвидации компании есть вероятность, что ее кадровые электронные документы утратят юридическую значимость. Законопроект № 1173189-7 призван прояснить: как хранить и передавать ЭД (в том числе с ЭП), как их конвертировать в бумажный вид и наоборот.

Формат подписи

Приказ Минтруда № 578н требует, чтобы электронная подпись была сформирована в соответствии с законом № 63-ФЗ. Этот закон указывает, что обязательный формат ЭП устанавливается «федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий...», создавая таким образом отсылку к приказу Минцифры от 14.09.2020 № 472 «Об утверждении формата электронной подписи, обязательного для реализации всеми средствами электронной подписи». Однако приказ № 472 содержит ошибки, например, в п. 6 перепутаны номера OID (объектный идентификатор), и не содержит полного объема информации, необходимой для формирования подписи, т.е. без дополнительных документов, которые не указаны в тексте приказа, сформировать подпись невозможно. Есть предположение, что недостающие в приказе

№ 472 данные для формирования подписи нужно заимствовать из IETF RFC 5652 (2009) или Р 1323565.1.025-2019 (Росстандарт), но какой конкретно прототип RFC (или европейский аналог) был использован как гарант совместимости, остается загадкой.

Чтобы сформировать совместимую подпись, разные ведомства вынуждены давать ссылки на конкретные зарубежные стандарты (ETSI TS 101 733), например «Требования к формату постановления..., вынесенных в форме электронного документа», утвержденные приказом ФССП России от 31.05.2022 № 350.

Открепляемая подпись

В приказе Минтруда № 578н кроме уже упомянутой отсылки к приказу Минцифры № 472 в неявном виде указывается, что с 01.03.2023 разрешена только открепленная подпись, т.е. «вроде бы» должен быть файл, содержащий только ЭД, и файл, содержащий только ЭП. Это можно считать первой мелью, на которую неожиданно для ответственного за КЭДО лоцмана сел уже находящийся в промышленной эксплуатации КЭДО с использованием прикрепленной ЭП. Для того чтобы сняться с этой «мели», может потребоваться дорогостоящая переработка уже внедренной системы. Регулятор на ходу существенно меняет правила, сужает круг разрешенных технологий, тем самым заставляя гадать: применение каких технологий будет ограничено завтра?

Из позитива: «вроде бы» не требуется сертификация средств СКЗИ при использовании НЭП; не требуется сертификация собственного неаккредитованного УЦ; не требуется, чтобы используемый КЭДО был включен в реестр отечественного ПО.

Помимо регуляторов в области ЭП – Минтруда, Роструда, ФСБ, Минцифры, Росстандарта (ответственного за ГОСТы и техрегламенты) – есть еще регуляторы в области защиты информации: ФСТЭК (сертификат соответствия ФСТЭК по требованиям безопасности информации) и Роскомнадзор. Работодатель является оператором персональных данных (ПДн) и в соответствии с законом № 152-ФЗ и его подзаконными актами (постановление Правительства РФ от 01.11.2012 № 1119, приказ ФСТЭК от 18.02.2013 № 21 и др.) обязан обеспечить в КЭДО выполнение длинного и постоянно расширяемого списка требований (например, закон № 266-ФЗ от 14.07.2022 требует перечисления криптографических средств, участвующих в обработке ПДн).

Если планируется развернуть собственный УЦ, то список проблем и сертификатов увеличивается вдвое.

Подпись длительного хранения

Основное ограничение на формат ЭП обусловлено необходимостью обеспечить юридическую значимость ЭД с ЭП при длительном (условно вечном) хранении. Проверка подписи и вывод об юридической значимости должны быть максимально очевидными в штатном (внесудебном) порядке и не требовать сложных экспертиз и расследований по признанию подписи. Сервисы проверки подписи, как встроенные в КЭДО, так и публичные (в отношении ЭД с КЭП), например на портале госуслуг, должны выдавать однозначный результат, включая проверку сертификата, на протяжении всего периода хранения подписанного документа.

При просроченном сертификате проверки ЭП большинство документов, подписываемых сейчас (усовершенствованных не выше CADES-T), не удовлетворяет этим условиям. Эти вопросы либо отдаются на откуп «третьей доверенной стороне», например, при обмене счетами-фактурами – оператору СЭД (он становится арбитром в спорных ситуациях), либо используются собственные «доверенные архивы», например, в рамках Указания Банка России от 25.11.2009 № 2346-У (бумажный ярлычок с контрольной суммой DVD подписывается от руки).

Возвращаемся к верификации сертификата ЭП при проверке подписи (тут и кроется основной подводный камень). Читаем закон № 63-ФЗ п. 2 ст. 11. Признание квалифицированной электронной подписи:

«2) квалифицированный сертификат действителен на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности указанного сертификата, если момент подписания электронного документа не определен».

Нас интересует только первая часть предложения, поскольку в общем случае на момент проверки сертификат однозначно будет недействителен: некоторые кадровые документы имеют срок хранения 75 лет, а некоторые (постоянного хранения) нужно хранить «вечно». В то же время срок действия личного сертификата обычно составляет 12–15 месяцев. Электронная подпись должна решить два вопроса (кроме проверки «математики» через расчет хеш-функции): доказательство момента подписания документа и действительности сертификата на момент подписания документа. Первый решается с помощью штампа времени, получаемого по протоколу TSP (Time-Stamp Protocol) от службы (сервера) штампов времени – доверенного субъекта инфраструктуры открытого ключа.

Если при проверке подписи выдается сообщение, что «математически» ЭП верна, но нет до-

верия к сертификату проверки подписи (например, истек срок его действия), то делается общий вывод: проверка выполнена с отрицательным результатом, документ не может считаться юридически значимым. Как обеспечить юридическую значимость документа на длительное время, для начала – на 10–15 лет?

Существует ошибочное мнение, что если подпись была сделана сертифицированным СКЗИ, то оно в обязательном порядке проверяет действительность сертификата и только после этого добавляет подпись, т.е. как бы усовершенствование подписи не требуется.

Основной (первый) вариант – это применение усовершенствованной подписи CADES-XL (CADES – X Long Type 1) и выше, которая от усиленной отличается добавлением в подпись доказательств действительности сертификатов на момент подписания. Это гарантирует сохранение юридической значимости ЭД при истечении срока действия сертификатов проверки подписи как самих подписантов, так и всей цепочки до сертификата корневого УЦ. При этом срок действия самого открытого ключа подписанта не важен: требуется только, чтобы ключ был действующим на момент подписания.

Доказательства включают штамп времени (TSP) и онлайн-проверку сертификата по протоколу OCSP (Online Certificate Status Protocol) либо проверку по списку CRL. В случае с OCSP помимо фиксации момента подписания результат онлайн-проверки статуса сертификата сохраняется в параметрах подписи. Типовой срок действия сертификата ключа подписи служб TSP и OCSP – 15 лет.

Альтернативой (вторым вариантом) может служить комбинация: сертификат проверки подписи на 15 лет и использование штампа времени (TSP, CADES-T). Доверенное время нужно для утверждения, что документ был подписан при действующем сертификате.

Проблема в том, что аккредитованные УЦ не желают выдавать сертификаты со сроком действия более 15 мес., хотя, согласно приказу ФСБ от 27.12.2011 № 796, можно установить срок 15 лет (ранее было 30 лет): «Срок действия ключа проверки ЭП не должен превышать срок действия ключа ЭП более чем на 15 лет».

Призывы к УЦ на порядок увеличить срок действия открытого ключа звучат регулярно, но пока пролонгированный срок предоставляют только специализированные УЦ, например, УЦ Банка России (12 лет).

При развертывании собственного неаккредитованного УЦ в зависимости от ограничений используемого криптопровайдера можно самостоятельно установить многолетние сроки на сертификат проверки подписи. Однако если документ одновременно будет подписан НЭП работника (максимум 15 лет) и КЭП работодателя (максимум 15 месяцев), то полученный выигрыш будет обнулен, поскольку по истечении минимального из сроков действия сертификатов любого подписанта юридическая значимость будет потеряна.

В обоих рассмотренных вариантах через 15 лет потребуется дальнейшее увеличение срока действия, т.е. дальнейшее продление юридической значимости кадровых документов. Обычно это делается перештамповкой: повторное усовершенствование ЭП до истечения срока действия сертификата проверки электронной подписи службы штампов времени – эдакий электронный нотариус-архивариус, продлевающий срок хранения ЭП на следующие 15 лет повторной штамповкой «архивным штампом» (CADES-A). Однако в текущих быстроменяющихся условиях есть вероятность того, что, когда дело дойдет до перештамповки (т.е. через 15 лет), требования к КЭДО или самой процедуре перештамповки будут совсем иными.

Таким образом, к двум вариантам – сразу при подписании обеспечить срок действия подписи 10–15 лет, т.е. CADES-XL или [CADES-T + «длинный» сертификат на 10–15 лет] добавляется вариант: спустя 15 месяцев (обычный сертификат) провести перештамповку CADES-A на 10–15 лет.

Если в КЭДО не используется ни один из приведенных вариантов, то в нем отсутствуют встроенные механизмы обеспечения долговременной юридической значимости документов, т.е. потребуется дополнительно использовать внешние механизмы, причем до прекращения действия сертификата, так как по истечении срока действия подпись из «кареты» мгновенно и безвозвратно превратится в «тыкву».

Слов «перештамповка» или отсылки к CADES-A в законодательном поле (и подполье) закона № 63-ФЗ не найти, и только находчивость лоцмана позволит «вроде бы» обеспечить долговременную юридическую значимость ЭД и ЭП. Приказ Минцифры России от 06.11.2020 № 580 «Об утверждении порядка создания и проверки метки доверенного времени» утверждает формат доверенного времени, но при этом не дает ясности по многим вопросам, например, какому международному формату (RFC/ETSI и его версии) соответствует и какова процедура сертификации сервера TSP (TSA, Time Stamping Authority).

Окончание статьи – в следующем номере «ИКС»

СВОБОДНЫЕ
ТЕХНОЛОГИИ
ИНЖИНИРИНГ

ПРОСТЫЕ РЕШЕНИЯ СЛОЖНЫХ ЗАДАЧ

ПРОЕКТИРОВАНИЕ И СТРОИТЕЛЬСТВО ДАТА-ЦЕНТРОВ

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

+7 (495) 120-28-66

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

Риски берем на себя

Как сегодня при создании ЦОДа минимизировать риски, связанные с использованием оборудования новых вендоров, и на какие технологии стоит ориентироваться? Ответы знает Евгений Колосков, технический директор компании «Свободные Технологии Инжиниринг».

– Какие вызовы и сложности возникли у проектировщиков и строителей ЦОДов в новых условиях?

– Первое, чего не хватает лично мне, – полноты обмена знаниями и опытом с зарубежными коллегами, информации о новых технологиях и технических решениях, мировых тенденциях. Раньше несколько раз в год выезжали на международные конференции, посещали передовые объекты в разных странах… Сейчас все это стало гораздо сложнее. Конечно, что-то можно почитать в интернете, но и там объем доступной нам информации сократился. И ничто не заменит живого общения.

Второе – уменьшение числа доступных технологий и числа поставщиков тех технических решений, что остались доступны. Недавно заполнял Карту вендоров (проект iKS-Consulting. – *Прим. ред.*) и понял, что если раньше мог назвать, скажем, около 20 вендоров систем энергетики, то сейчас ограничусь пятью и, скорее всего, остановлюсь на трех. Выбор стал существенно уже.

Третье – разрыв логистических цепочек, непредсказуемость сроков поставки. Вот оборудование вроде в наличии, на складе, но его перекупают, и оно исчезает. Это создает неопределенность в планировании сроков реализации проектов.

Наконец, четвертое – рост себестоимости технических решений и общих затрат на проекты. Особенно это существенно для тех проектов, бюджет которых составлялся по старым курсам валют.

– Можно ли сказать, что отрасль ЦОДов уже сформировала новый vendor list, или процесс еще не закончен и изменения продолжаются?

– Пока все в динамике. Сегодня в ЦОДах начали использовать оборудование тех производителей, в сторону которых раньше даже не смотрели. Многие заказчики сталкиваются с тем, что им на своих площадках приходится экспериментировать. Если говорить о китайских вендорах, то они весьма специфичны во многих отношениях. Кроме того, в России климат, требования к комплектации, паспортизации, программам подбора иные, чем те, что сложились в азиатском регионе. Программное обеспечение должно быть русифицировано, а интерфейс приведен к виду, привычному для наших специалистов. Да и алгоритмы управления нуждаются в отладке. Готовых таких решений нет, они создаются в процессе совместной работы с производителями.

В каждом новом проекте появляются новые производители, новые решения. Более того, наталкиваешься на подводные камни в продукции тех вендоров, с которыми, казалось бы, уже давно знаком. При проектировании по документации все нормально, а в процессе пусконаладки возникают проблемы, которые изначально были совсем не очевидны. Одни вендоры помогают в таких ситуациях, другие – нет. Соответственно последние вычеркиваются из списка возможных поставщиков.

– Да, экспериментировать в ЦОДе – это неправильно. Как снять риски с заказчиков?

– Все риски ложатся на нас как генпроектировщика и генподрядчика. На построенный объект мы можем дать пятилетнюю гарантию, плюс мы несем обязательства по пусконаладке и опытной эксплуатации. На отдельные компоненты систем дает гарантию завод, обычно 12 или 18 месяцев с момента поставки на объект. Но при работе с новыми производителями чаще всего просим их предоставить расширенную гарантию.

Мы стараемся не экспериментировать с оборудованием тех производителей, чья продукция ранее в ЦОДах никогда не эксплуатировалась. Особенно это касается основных систем – ИБП, ДГУ, чиллеров, кондиционеров. Даже если завод имеет большой опыт изготовления схожих систем, но не для ЦОДов. Например, всегда делали холодильное оборудование для катков, и вот решили выпустить чиллер для ЦОДов. Мы понимаем специфику функционирования такого оборудования в ЦОДах. Есть много нюансов в алгоритмах работы, и для их оптимизации нужен опыт.

Поэтому ориентируемся на системы, которые ранее уже были инсталлированы в ЦОДах, не обя-

зательно российских, и для обслуживания которых есть сервисные центры. Оборудование должно быть ремонтопригодно, компоненты доступны и заменяемы.

Если приходится устанавливать оборудование, которое производитель делает по нашим заказам впервые, то оно должно иметь простую и понятную компонентную базу, и мы тщательно тестируем его на заводе. Так, с несколькими производителями разработали решение для холодных стен в качестве замены прецизионным кондиционерам. Протестировали, убедились, что все работает, теперь заказываем партию для проекта.

– К параллельному импорту не прибегаете?

– Только в экстренных случаях. Предположим, у заказчика было 11 комплектов оборудования, а для того чтобы запустить ЦОД, нужно 13 комплектов. Разумеется, мы эту проблему решим, привезем и установим недостающие комплекты. Но в качестве основного решения параллельный импорт не рассматриваем.

– Как замена вендоров и другие обстоятельства изменили выбор технологий? Откатились ли мы назад в технологическом плане?

– Да, по многим технологиям откатились. Например, приходится отказываться от современных чиллеров с компрессорами Danfoss Turbocor. Это хорошее решение для ЦОДов. Конечно, чиллер такой из Китая привезут. Но отдельно эти компрессоры доступны только по параллельному импорту – очень велики риски. Но ничего страшного: используем чиллеры с поддержкой естественного охлаждения (фрикулинга) на более простой компонентной базе. Их делают и в России.

Другой пример – решения с воздушным фрикулингом, с большими вентиляционными установками. Здесь возникают проблемы с контроллерами. Поэтому на данном этапе стараемся такие решения в проекты не закладывать.

Так сказать, немного осторожничаем с выбором решения. Стараемся применять то, что привычно, точно будет работать, можно отремонтировать. Может быть, энергоэффективность у такого решения будет чуть хуже, чем у суперсовременного, но для ЦОДов важнее надежность и устойчивость.

– А как более низкое качество (надежность) продукции новых вендоров можно компенсировать на уровне проектирования (архитектуры)? Повысить уровень резервирования или какими-то другими способами?

– Например, в системе энергоснабжения мы стараемся не использовать оборудование большого номинала. Тогда и логистика проще, и сроки производства меньше, и с экономической стороны часто получается выгоднее. А главное, не сужается выбор производителей. Ведь чем мощнее оборудование, тем меньше его поставщиков на рынке. Взять, скажем, ДГУ: установки мощностью 2500–2600 кВт есть максимум у трех поставщиков.

В архитектуре избыточного резервирования, сверх необходимого, обычно не предусматриваем. Но если знаем, что у какого-нибудь компонента долгий срок поставки, то его закладываем в ЗИП. Раньше так не делали. А сейчас пусть лучше хранится у заказчика на объекте.

– Индустрия уже привыкла к хорошему – проектировать в BIM. Какова ситуация с BIM-системами? Пришлось ли их менять? Есть ли достойные российские системы?

– BIM – это большой комплекс компонентов. Что касается программ, в которых работают проектировщики, то в России полноценной замены пока не видим. Хотя внимательно отслеживаем ситуацию, взаимодействуем со всеми основными игроками этого рынка. Сегодня работаем на старом европейском софте, но проблем в плане организации рабочего места специалиста по проектированию ЦОДов не ощущаем.

А вот программы для хранения моделей, совместной работы разных специалистов, доступа к моделям разных участников и т.д. есть отечественные, и мы их используем. То есть можно создать модель в импортном ПО, а работать с ней с помощью российского.

– Мировые вендоры предоставляли BIM-модели своих продуктов. Есть ли такие модели у новых вендоров?

– Мало кто из производителей сам разрабатывал цифровые модели своих устройств. Обычно заказывали специализированным компаниям. Так поступают и российские производители. Новых вендоров из Китая мы просим подготовить модели, и обычно они идут нам навстречу. В принципе ничего не изменилось.

Кроме того, при наличии специалиста по BIM можно достаточно быстро переделать модели оборудования одного производителя на схожие другого.

– Традиционный вопрос о кадрах. Как решаете проблему? Где берете квалифицированных проектировщиков?

– Дефицит кадров инженерных специальностей был всегда, сейчас он только усилился. Готовых специалистов нет, точнее, они все заняты. Поэтому приглашаем инженеров, которые раньше ЦОДы не проектировали. Обучаем, показываем построенные и строящиеся объекты. Также активно сотрудничаем с МЭИ. В планах выстроить взаимодействие и с другими вузами. Мы считаем, что по своему профилю этот вуз ближе всего к нашей специализации. Подготовили программу обучения, организуем практику для студентов, приглашаем молодых специалистов на работу. Это относится не только к проектировщикам, но и к специалистам службы эксплуатации ЦОДов.

А специалистов требуется все больше, поскольку проектов тоже становится больше с каждым годом. Да, какие-то технологии теперь недоступны, но проектирование ЦОДов от этого не стало менее интересным, это творческий, захватывающий процесс. Работать стало сложнее, но мы любим свою работу и стараемся делать ее качественно.

Системы охлаждения ЦОДа. Поворот «все вдруг»

Александр Барсков

Сменив поставщиков комплектующих и оправившись от аврала, вызванного взрывным ростом числа заказов весной 2022 г., российские производители систем охлаждения переходят в нормальный режим работы и вместе с китайскими коллегами формируют новый вендор-лист для российских ЦОДов.

Системы охлаждения – ключевой элемент инженерной инфраструктуры ЦОДов – обычно становятся одной из основных тем для обсуждения на организуемых «ИКС-Медиа» конференциях DCDE. Однако на конференции, прошедшей в мае 2023 г., в фокусе внимания оказались не технологии, а организационные вопросы.

Весной-летом 2022 г., с уходом из России многих западных вендоров, на отечественных производителей систем охлаждения обрушился вал заказов. «В первый момент они захлебывались, долго отвечали на запросы. Столкнулись с необходимостью переориентации на новую базу комплектующих, вынуждены были заменять программы подбора оборудования, перестраивать логистику – и все это негативно сказалось на сроках производства. Но ведущие компании справились, продолжают успешно выпускать и поставлять продукцию», – подвел итоги года работы в условиях жестких санкций Виктор Гаврилов, технический директор компании «АМДтехнологии».

К основным отечественным производителям систем охлаждения для ЦОДов можно отнести давно присутствующие на этом рынке компании «Рефкул», «КБ Борей», «Вайбос», «Веза», «Купол», а также Systeme Electric – реинкарнацию российских активов Schneider Electric. Появились и совсем новые компании. Например, «ТехноФрост», традиционно работавшая на рынке оборудования для промышленного холода, начала осваивать рынок ЦОДов, выпустив «очень неплохие», по мнению В. Гаврилова, чиллеры и шкафные кондиционеры. Также он отметил, что развивать свои продуктовые линейки в направлении чиллеров и шкафных кондиционеров для ЦОДов стали и компании, занимавшиеся изготовлением вентиляционного оборудования.

Что касается европейских производителей, то, по данным В. Гаврилова, в Россию по-прежнему поставляется оборудование нескольких известных итальянских брендов (причем объем продаж в прошлом году был довольно большим), а также ряда турецких вендоров. Отметил эксперт и малазийскую компанию Dunham-Bush.

На восточном фронте

Отдельно следует упомянуть целую армию китайских поставщиков: Airsys, Attom, Coolnet, Envicool, Hairf, Kstar, Leming, Midea Group, Shenling, TICA и др. Большинство китайских производителей ориентируются на поставки шкафных и внутрирядных кондиционеров. Холодильные машины большой мощности, востребованные в крупных ЦОДах, есть далеко не у всех. Любопытно, что в самом Китае на рынке климатического оборудования для ЦОДов лидирует не китайский вендор, а европейская Vertiv (доля 15,1%). Далее идут две китайские компании – Envicool (13,6%) и Huawei (10%), а на четвертом месте снова европейская – Stulz.

> В 2022 г. на отечественных производителей систем охлаждения обрушился вал заказов. Параллельно они столкнулись с необходимостью переориентации на новую базу комплектующих и перестройки логистики – и все это негативно сказалось на сроках производства.

Говоря об оборудовании ряда китайских вендоров, В. Гаврилов посетовал на сложности его подбора для конкретных проектов. Западные вендоры руководствуются стандартами Eurovent Certita Certification и указывают производительность своих продуктов при расчетной температуре воздуха на входе в кондиционер 24°C. Китайские же компании указывают производительность при разных температурах, что усложняет сравнение и выбор оборудования. Кроме того, далеко не все китайские производители указывают, на какую температуру конденсации их оборудование рассчитано. Наконец, у российских заказчиков и китайских поставщиков может быть разное понимание того, что такое низкотемпературный комплект.

Компания Envicool, номер два на китайском рынке прецизионных кондиционеров – один из немногих китайских производителей, если не единственный, имеющий официальный офис

Сравнение климатического оборудования российских и китайских производителей. Обобщенные данные ▼

Критерий сравнения	Оборудование российского производства	Оборудование китайского производства
Наличие технической документации, каталоги, чертежи	Частично, в основном на ранее выпущенное оборудование	Документация имеется, но не у всех производителей в полном объеме
Программа подбора оборудования	В стадии разработки, есть пилотные версии. Подбор по запросу	ПО имеется у производителей, но проектным организациям не предоставляется. Подбор по запросу
Время обработки запроса, дней	1–10	1–2 на стандартное оборудование
Наличие официального представительства	Да, завод	Нет, только дистрибьюторы
Наличие сервисных центров	Да, завод, сертифицированные партнеры	Сервисная поддержка дистрибьюторов, частично сертифицированные партнеры
Адаптация оборудования для климата РФ	Да, на уровне производителя	На уровне специальных опций, низкотемпературных комплектов

Источник: «АМДтехнологии»

в России. Причем, как рассказал Владимир Шепелев, управляющий директор этого офиса, в нашу страну компания уже поставила более 10 тыс. единиц оборудования (около 700 прецизионных кондиционеров). В своих решениях Envicool использует компоненты ведущих брендов, что, как подчеркнул В. Шепелев, может оказаться особенно важным в текущих условиях: например, компрессоры и вентиляторы западных производителей, к которым привыкли заказчики, напрямую в России ввозиться не могут, а в составе кондиционеров Envicool поставляются.

> Заказчики, ранее работавшие с западными вендорами, привыкли получать «все и сразу», включая полную проектную документацию, качественные программы подбора, развитое сервисное обслуживание. Многим российским компаниям это только предстоит реализовать.

В основном российским заказчикам компания предлагает традиционные решения для периметрального и внутрирядного охлаждения. Однако в портфеле Envicool есть и другие продукты – например, системы с косвенным испарительным охлаждением, холодные стены, комплексы прямого фрикулинга и решения с жидкостным охлаждением.

Окно возможностей для российских производителей

То, насколько напряженным выдался 2022 г. для российских производителей, хорошо иллюстрируют данные, которые привел генеральный директор компании «Рефкул» Алексей Морозов: «За год мы рассчитали 1137 проектов. Причем это не подбор кондиционеров в соответствии с заданными характеристиками машзала, а пересчет проектов, в которые изначально было заложено оборудование ушедших вендоров – Stulz, Vertiv, Uniflair. Заказчики просили выдержать те же габариты, сделать такую же подводку труб и т.д.». В результате конструкторы компании разработали 70 новых единиц продукции (без учета различных модификаций). Параллельно заводу пришлось полностью менять почти всю компонентную базу: компрессоры, вентиляторы, теплообменники.

Холодная стена Envicool ▼

Сегодня «Рефкул» производит полный набор решений для охлаждения: моноблочные, межрядные и шкафные кондиционеры (как «на фреоне», так и «на воде»), а также чиллеры холодопроизводительностью до 3500 кВт. Суммарная холодопроизводительность выпущенной в прошлом году климатической техники – около 90 МВт. Из этого объема примерно 60–65%, а именно 212 прецизионных кондиционеров и 80 чиллеров, ушло в ЦОДы.

В текущем году выпуск значительно увеличится. Только прецизионных кондиционеров будет изготовлено не менее 500 единиц (на это количество контракты уже подписаны). Запланировано создание чиллеров на центробежных компрессорах. В октябре предприятие начнет сооружение второй очереди общей площадью 8 тыс. кв. м. Завершить строительство намечено к весне 2024 г. Наконец, в 2023 г. «Рефкул» построит испытательную камеру, в которой можно будет тестировать прецизионные кондиционеры с расходом воздуха до 200 тыс. куб. м и чиллеры длиной до 12,5 м.

«Если до 2022 г. мы существовали “вопреки”, то сейчас стало легче», – рассказал Ратмир Трошин, директор по развитию бизнеса «КБ Борей». Компания выпустила свой первый коммерческий продукт – внутрирядный кондиционер «на воде» – в 2019 г. Затем разработала и запустила в производство чиллеры. В прошлом году, «поняв, что рынок освободился», начала разрабатывать фреоновые системы и изготавливать соответствующие внутрирядные и шкафные кондиционеры. Также недавно «КБ Борей» расширила линейку чиллеров с фрикулингом, в которую сейчас входят аппараты до 520 кВт. Особенность оборудования компании – использование контроллера собственной разработки, а также инверторных компрессоров исключительно компании Danfoss.

На основе своей системы прецизионного кондиционирования на охлажденной воде с фрикулингом «КБ Борей» также разработала несколько моделей мини-ЦОДов BMD. Использование этого решения, имеющего шумоизолированный герметичный корпус (класс защиты IP 65), позволяет максимально снизить требования к строительной подготовке помещений для установки ИКТ-оборудования и, как следствие, се-

▲ Сборочный цех завода «Рефкул»

бестоимость и сроки реализации проектов. Система кондиционирования способна отвести 4–12 кВт (в зависимости от модели) тепла, выделяемого размещенным в мини-ЦОДе оборудованием. Способ охлаждения оборудования (не требующий установки вентиляторов в шкафу) запатентован, причем патент признан в 15 странах Евросоюза.

Патентная заявка подана и на новинку – уличный всепогодный мини-ЦОД УВП 8 (на 8 кВт), который позволяет создать необходимую серверную инфраструктуру под открытым небом. Система состоит из минимум одного герметичного изолированного телекоммуникационного шкафа и одного модуля кондиционирования воздуха с функцией естественного охлаждения, причем воздух из окружающей среды не попадает внутрь шкафа. Модульность конструкции дает возможность объединять телекоммуникационные шкафы и модуль кондиционирования в единый конструктив (ряд) для увеличения емкости и мощности мини-ЦОДа, а также для резервирования системы кондиционирования.

Когда ждать полностью российский кондиционер

Российским производителям сейчас не просто. Заказчики, ранее работавшие с западными вендорами, привыкли получать «все и сразу», включая полную проектную документацию, качественные программы подбора, развитое сервисное обслуживание и т.д. Поскольку наши предприятия зачастую разворачивают производство оборудования с нуля – на новой компонентной базе, по новым требованиям, – то обеспечить все это могут не всегда. Нередко в спешке выпускают «сырой» продукт. Но если производитель вовремя реагирует и исправляет недоработки, это уже хорошо.

Сегодня российские предприятия используют в основном зарубежные комплектующие, в том числе базовые элементы систем охлаждения – вентиляторы и компрессоры. Но появились перспективы перехода к полноценному локальному производству. В конце октября 2022 г. Минпромторг России приказом № 4516 утвердил План мероприятий по импортозамещению в отрасли экологического машиностроения до 2024 г. Этот план предусматривает разработку собственной компонентной базы для промышленного холодильного и вентиляционного оборудования, включая компрессоры (холодопроизводительностью 5–3000 кВт), теплообменники, терморегулирующие вентили, соленоидные клапаны, предохранительные и регулирующие клапаны, компактные осевые вентиляторы с AC- и EC-двигателями. На это выделены необходимые денежные средства. Конечно, не через год-два, но в перспективе 10 лет есть надежда увидеть в ЦОДах полностью российские кондиционеры и чиллеры. ИКС

▲ Межрядный фреоновый кондиционер «КБ Борей»

Пора возвращаться к комплексным решениям

Быстро наполнив продуктовый и сервисный портфель, компания Systeme Electric готова стать лидером рынка инженерной инфраструктуры ЦОДов. Роман Шмаков, первый заместитель генерального директора по рынку «ИТ-решения» и сервису, убежден, что именно комплексные решения – ключ к успеху.

– Как вы оцениваете текущий этап развития российской отрасли ЦОДов, основные тенденции?

– В отрасли ЦОДов наблюдается, я бы сказал, дуализм. Если раньше рынок развивался благодаря перетеканию заказчиков из собственных корпоративных ЦОДов в коммерческие, рос спрос на colocation и облака, а потребность в собственной инфраструктуре снижалась, то сейчас повышенная активность наблюдается в обоих сегментах – и коммерческих, и корпоративных дата-центров. Даже те заказчики, которые ранее закрывали площадки и переходили на аутсорсинг, сейчас возрождают свою инфраструктуру. Это следствие общего снижения уровня доверия к внешним сервисам. Риски операторов коммерческих ЦОДов возросли, они сильно зависят от экосистемы, включая поставщиков аппаратного обеспечения и ПО.

Заказчики стали страховаться, развивать свои площадки, больше строить, а также усиливать собственную экспертизу в области эксплуатации инфраструктуры. Но при этом внешние сервисы используют не меньше, зачастую задействуют их для дублирования критических функций. На рынке коммерческих ЦОДов также наблюдается взрывной рост, который усиливается практически полным отсутствием доступа к зарубежным сервисам. Все традиционные участники рынка коммерческих ЦОДов и новые игроки заявляют о планах строительства, расширения площадок.

Еще один важный тренд – децентрализация. Многие заказчики проявляют интерес к переносу инфраструктуры за пределы Москвы, в том числе для резервирования. Надо отметить, что и качество региональных площадок за последние годы существенно повысилось. Кроме того, зачастую затраты на построение региональных ЦОДов ниже.

– Рынок решений для инженерной инфраструктуры претерпел кардинальные изменения. Насколько он близок к стабилизации?

– Рынок далек от стабилизации. В прошлом году, когда были нарушены логистические цепочки и привычный ассортимент, он напоминал Дикий Запад.

Но я вижу хорошие качественные изменения. На прошедшем в конце мая Инновационном саммите, где мы представляли решения для разных рынков, многие заказчики говорили о потребности в долгосрочных партнерствах. Они стали четко различать поставщиков, т.е. тех, кто может что-либо быстро найти и привезти, и вендоров – компании, которые предоставляют поддержку полного цикла: не только поставку, но и маркетинг, предпродажную подготовку, дальнейшее сопровождение, сервис и обучение. Именно по этой модели работает Systeme Electric. Наша стратегия – полностью поддерживать заказчиков на всех этапах жизненного цикла продуктов и решений – все более востребована.

– К сожалению, после определенного периода оптимизма по поводу импортозамещения у многих заказчиков наступила стадия пессимизма, связанная с невысоким качеством решений. В чем причина этого?

– Понятие «российский производитель» в какой-то степени размыто. Некоторые компании, называющие себя отечественными производителями, полноценно продукт в РФ не производят, в лучшем случае адаптируют. Ну а те, кто реально производят, столкнулись со сложностями.

На мой взгляд, главная из них – это проблема роста. Те, кому не удалось масштабировать свою работу, чтобы соответствовать спросу, могли поставлять продукцию без должного внимания ко всем параметрам. В результате заявления производителей расходились с ожиданиями заказчиков.

– Systeme Electric быстро наполнила портфель продуктов до уровня, который был у Schneider Electric в России. Как вам это удалось? Не сказалась ли высокая скорость вывода продуктов на рынок на их качестве?

– Вопрос качества продукции для Systeme Electric – приоритетный. Наша компания стала одной из первых, кто взял курс на локализацию еще в 2014 г.

С тех пор большая часть продуктов производится в РФ, поэтому все процедуры контроля качества давно отлажены. Если говорить о продукции, которая по нашим ТЗ изготавливается за границей, то наша команда обладает всеми необходимыми компетенциями. Кроме того, некоторые наши продукты производятся на фабриках, с которыми мы сотрудничаем много лет.

Мы осознанно затратили много времени на выведение новых продуктов именно для того, чтобы обеспечить соответствие качества продукции нашим требованиям и стандартам российского рынка.

Качество продуктов и решений закладывается не только на этапе проектирования и производства, но и на протяжении всего их жизненного цикла – за счет профессионального управления и поддержки. Мы уделяем этому большое внимание.

– Если можно, расскажите, где находятся основные производственные мощности.

– Около 60% продукции производится в РФ. Остальное – преимущественно в странах Азии: в Китае, на Тайване и в Малайзии. Это известные производственные площадки, с которыми у нас многолетние партнерские отношения. Но наша стратегия – повышение доли локальных продуктов. Мы продолжаем активно работать над развитием производства в РФ.

– Schneider Electric, точнее APC, всегда была признанным лидером рынка ИБП. Какие продукты должны помочь вам сохранить лидерские позиции?

– Да, для нас ИБП – особенная, флагманская категория. Это касается и однофазных, и трехфазных аппаратов. Предлагаемые нами сейчас продукты по отдельным показателям превосходят даже легендарные продукты APC. У нас появилось больше гибкости в производстве, чтобы обеспечить потребности российского рынка.

В свое время ИБП APC во многих сегментах стали стандартом. В их числе – модульные трехфазные ИБП Symmetra. Недавно мы представили наш флагман в этой категории – ИБП Excelente для критически важной инфраструктуры, включая ЦОДы. В ближайшее время планируем вывести на рынок специализированные варианты этих ИБП для различных индустрий – нефтегаза, атомной промышленности, производственных площадок.

– Также Schneider Electric первой предложила полное (комплексное) решение для инженерной инфраструктуры ЦОДов. Сегодня у вас есть такое предложение?

– Мы стремимся не только предлагать качественные высокопроизводительные продукты, но формировать экосистему, включая сервисы и приложения. Такая экосистема продуктов и решений получила название SystemeOne. Комплексные решения дают серьезные преимущества с точки зрения совместимости, управляемости, прогнозирования и масштабирования инфраструктуры и опираются при этом на российское программное обеспечение.

Отмечу, что мы создали единую среду, которая не просто связывает продукты Systeme Electric, но и обратно совместима с оборудованием APC в решениях InfrastruXure как на физическом, так и на программном уровне. Например, серверные шкафы Uniprom Rack имеют те же габариты и объединяются в ряды с APC NetShelter SX. А система централизованного мониторинга APC Data Center Expert, установленная у многих наших заказчиков, автоматически распознает большинство новых продуктов Systeme Electric для ЦОДов, например, Uniprom Rack PDU. Это позволяет заказчикам совершенствовать свою инфраструктуру как путем замещения, так и путем дополнения новыми продуктами и решениями Systeme Electric.

– Комплексное решение – это не только портфель продуктов, но и набор сервисных услуг. Что вы сейчас предлагаете заказчикам?

– Мы не только сохранили сервисное предложение Schneider Electric, но и пошли существенно дальше. Как независимая компания мы оказываем более широкий спектр услуг комплексного обслуживания инфраструктуры заказчика. Причем они охватывают оборудование не только Schneider Electric и Systeme Electric, но и других производителей. Заказчики, которые используют оборудование покинувших рынок вендоров, очень заинтересованы в профессиональных сервисах эксплуатации и модернизации, которые обеспечивают непрерывность бизнес-процессов. Именно эту задачу мы решаем.

– Кого видите основным конкурентом на рынке решений для инженерной инфраструктуры ЦОДов? Какую долю планируете занять на нем, когда ситуация стабилизируется?

– В продуктовом поле – это компании, которые производят неплохие продукты. Но если говорить о комплексном подходе, то уникальность стратегии Systeme Electric – в предложении заказчику наиболее широкого продуктового и сервисного решения.

Скорее, наш «конкурент» – общее снижение уровня доверия к поставщикам на фоне ситуации на рынке в предыдущие месяцы. Но мы опираемся на нашу стратегию и конкретные факты. Поэтому все больше компаний соглашаются с тем, что пора возвращаться к подходу, основанному на комплексных решениях.

Наша компания исторически была лидером на рынке инженерной инфраструктуры ЦОДов. И стратегия Systeme Electric – это стратегия лидерства. Считаю, что у нас есть все предпосылки для того, чтобы выйти на лидерские позиции, продолжая развивать портфель востребованных рынком продуктов и сервисов.

Екатеринбург 28 ноября 2023

Hyatt Regency Ekaterinburg

На конференции традиционно рассматриваются вопросы развития индустрии дата-центров и облачных сервисов на территории УФО, а также основные аспекты создания и эксплуатации ЦОДов.

- Новые драйверы развития ЦОДов в регионах
- Инженерная и ИТ-инфраструктура дата-центров
- Облачные технологии и сервисы
- Edge-ЦОДы для различных сегментов экономики

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

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

Реклама 16+

ОРГАНИЗАТОРЫ ИКС МЕДИА iKS CONSULTING

ПРИ ПОДДЕРЖКЕ И УЧАСТИИ КООРДИНАЦИОННЫЙ СОВЕТ ПО ЦОДам И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ Автономная некоммерческая организация

Найди свой ЦОД: чек-лист для потенциальных клиентов

Анастасия Нойманн,
директор по продажам;
Дина Нуркаева,
директор по маркетингу,
IXcellerate

Выбор коммерческого дата-центра для размещения серверного и сетевого оборудования – задача нетривиальная. Площадки отличаются друг от друга размерами, местоположением, уровнем надежности, энергоэффективностью и множеством других параметров. Как не потеряться в этом разнообразии?

Дата-центры давно перестали быть прерогативой крупных корпораций. К их услугам прибегают не только экономические гиганты, но и небольшие компании. В одной только Москве существует более 80 крупных дата-центров, в Санкт-Петербурге – около 30. Размещение оборудования в дата-центре снижает стоимость эксплуатации ИТ-ресурсов и повышает безопасность хранения информации. Тем не менее у каждой компании свои задачи и свои требования к ЦОДу, которые определяются масштабом и спецификой ее бизнеса. Например, для запуска процессингового центра банка, базирования критически важных серверов крупного маркетплейса, организации резервного ИТ-кластера или хостинга сайта-визитки нужны разные уровни компетенций и инфраструктурной оснащенности.

Безусловно, необходимый этап поиска – анализ рынка: изучение рейтингов, рекомендаций, ценовых предложений, очное знакомство и т.д. Но изучить предложения и посетить 20 и даже 10 дата-центров – процесс долгий и трудоемкий. Возможно, вашим критериям соответствуют всего три или пять объектов, но как их выявить?

Чтобы сузить круг кандидатов, нужно сформулировать свои ожидания и требования к потенциальному ЦОДу и, исходя из них, решить, какие параметры для вас критически важны, а какие второстепенны. Оптимизировать процесс поиска и сделать правильный выбор поможет чек-лист – список вопросов, который впоследствии ляжет в основу технического задания.

Вопрос 1. Какой объем оборудования вы собираетесь разместить в коммерческом ЦОДе? Планируете ли вы в дальнейшем расширять свое присутствие на внешней площадке?

Если речь идет о больших масштабах, круг поиска будет ограниченным, особенно если ваша компания быстро развивается и в будущем вы планируете наращивать серверную и сетевую инфраструктуру за пределами офиса. Задавая вопрос о наличии свободных стойко-мест, нужно интересоваться не только текущей емкостью дата-центра, но и его стратегическими планами, а также историей. Если коммерческий ЦОД постоянно строится и расширяется, имеет надежных инвесторов и программу дальнейшего развития – это серьезный аргумент за то, чтобы включить его в список кандидатов.

Поэтому прежде всего нужно выяснить размер ЦОДа: площадь, количество машинных залов и свободных стойко-мест, а также возможности масштабирования объекта – способность дата-центра удовлетворить не только текущие, но и будущие потребности в услугах colocation.

Вопрос 2. Какое именно оборудование вы собираетесь размещать?

Одно дело, если у вас лишь несколько серверов стандартной конфигурации, и совсем другое, если вам нужно поддерживать высоконагруженную СУБД, ядро сети, а возможно, и облачную платформу. На-

сколько мощное у вас оборудование? Далеко не каждый дата-центр располагает инфраструктурой с гарантированным энергоснабжением до 25 кВт на стойку. Если уровень инженерной инфраструктуры ЦОДа не соответствует планируемым нагрузкам, сбоев в подаче электроэнергии и работе системы кондиционирования не избежать.

В большинстве случаев при проектировании ЦОДа его энергомощность определяется, исходя из прогнозируемого энергопотребления в расчете на одну стойку. Если ваши стойки достаточно высоконагруженные (10 кВт и выше), выбор сузится довольно быстро, а если, наоборот, с невысоким потреблением, то незачем переплачивать за ненужные мощности.

Таким образом, второй критерий выбора ЦОДа – его энергомощность, возможность подключать оборудование для сверхплотных вычислений. Для этого объект должен располагать соответствующей инфраструктурой и большим запасом резервных мощностей.

Вопрос 3. Где расположен объект? Как далеко он находится от вашего офиса? Соответствует ли его расположение нормам строительства ЦОДов?

Для многих клиентов расстояние от офиса до площадки имеет принципиальное значение: они хотят иметь возможность в любой момент добраться до дата-центра быстро, в том числе общественным транспортом.

Кроме того, местоположение – весомый фактор как для бюджета, так и для безопасности оборудования и хранящихся на нем данных. С одной стороны, чем дальше ваш офис и дата-центр находятся друг от друга, тем дороже обойдется аренда каналов связи. С другой стороны, чем дальше ЦОД от резервной площадки, тем устойчивее вся ИТ-система.

Подыскивая ЦОД, нужно внимательно изучить его «окружение». Дата-центр не должен находиться вдали от транспортных магистралей, чтобы не затруднять доступ к оборудованию и не раздувать бюджет на строительство или аренду каналов. Вместе с тем есть жесткие правила, согласно которым ЦОДы должны располагаться в местах, удаленных от аэропортов, военных баз, топливохранилищ и других объектов критически важной для города инфраструктуры. Если поблизости от дата-центра прорвет городской теплоотвод, это может грозить затоплением и порчей оборудования. Также нежелательно, чтобы ЦОД находился в офисном здании. Оптимальным вариантом считаются дата-центры, расположенные в отдельно стоящих промышленных сооружениях.

Поэтому, выбирая между качеством услуг дата-центра и его близостью, вам, возможно, придется принять компромиссное решение. Если же у подходящего по качеству услуг и другим параметрам провайдера в управлении не один, а несколько объектов, это значительно упростит поиск территориально приемлемой площадки.

Вопрос 4. Какое время непрерывной работы (uptime) подходит для решения ваших задач?

Условия договора с коммерческим ЦОДом предусматривают максимально возможное время простоя инфраструктуры из-за аварии или перебоев в электроснабжении. Этот параметр напрямую связан с надежностью дата-центра и может сильно варьироваться. Например, провайдер IXcellerate гарантирует доступность своих услуг (показатель отказоустойчивости) на уровне не менее 99,982%, что означает не более 95 мин простоя в год. Чем выше показатель отказоустойчивости, тем лучше защищены ваши данные.

Если у вас в команде есть достаточное количество профильных экспертов, надежность объекта можно оценить собственными силами. Можно привлечь для этой задачи внешних консультантов, а можно довериться сертификатам независимых аудиторов, которые по инициативе оператора ЦОДа оценивают его соответствие международным нормам и присваивают тот или иной уровень надежности. Система классификации представляет собой метод оценки объектов на основании ожидаемой производительности и безотказности их работы и имеет четыре уровня (Tier/Class/Rate):

- Tier I – базовая инфраструктура без резервирования (доступность сервиса – 99,671%);
- Tier II – инфраструктура с резервными мощностями только для активного оборудования (доступность сервиса – 99,749%);
- Tier III – полное резервирование инфраструктуры без прерывания работы на время ремонта (доступность сервиса – 99,982%);
- Tier IV – отказоустойчивая инфраструктура, в которой используются двойное резервирование и дублирование рабочей системы (доступность сервиса – 99,995%).

В случае аварии, например, потери одного или сразу обоих энерговводов, в дата-центрах уровня III и IV включатся дизель-генераторы, и дата-центр продолжит работу в автономном режиме до тех пор, пока проблема не будет устранена.

Выбор дата-центра того или иного уровня Tier зависит от требований к отказоустойчивости, от того, насколько критичны для компании воз-

можные перерывы в работе и доступность данных. Необязательно переплачивать за максимальную надежность сервисов ЦОДа, если компания в состоянии справиться со случайным сбоем сервера в нерабочее время. Но если ваш бизнес функционирует круглосуточно и любой простой может привести к уходу клиентов и финансовым потерям, выбор высоких уровней уже оправдан.

Вопрос 5. Как обеспечивается коннективность? Какие задачи в сфере телекоммуникаций или обмена трафиком нужно решать с помощью ЦОДа?

Одна из ключевых характеристик дата-центра – это качество связи. Доступность ЦОДа и высокоскоростные соединения уже стали практически нормой для любого бизнеса. Большинство дата-центров резервируют линии связи за счет установления соединений с двумя или тремя операторами на случай сбоев. Но этого достаточно далеко не всем. Для компаний, оперирующих большими объемами данных, необходимы более надежные и разнообразные сетевые соединения с внешним миром – серверами своих клиентов, партнеров, провайдеров облачных сервисов и т.д.

Высокий уровень связности (коннективности) обеспечивается за счет присутствия в ЦОДе большого количества операторов связи и точек обмена трафиком. Нейтральность дата-центра – или его независимость от какого-либо конкретного оператора – дает его клиентам возможность выбора и подключения к множеству различных сетей и провайдеров телеком-услуг.

Доступ к большому «маркетплейсу» услуг связи позволяет клиентам нейтрального ЦОДа решать любые задачи в сфере телекоммуникаций – строить гибридные ИТ-инфраструктуры, подключать облачные сервисы, предоставлять услуги на мировом уровне, а также локализовать трафик и сервисы в соответствии с особенностями региональных рынков.

Вопрос 6. Как организована защита дата-центра от возможных угроз?

Говоря о безопасности ЦОДа, мы имеем в виду его защиту как от виртуальных, так и от физических угроз.

Виртуальная безопасность – это наличие административных регламентов и технических средств защиты от любых кибератак. К первым относятся правила доступа посторонних лиц на площадку, ко вторым – системы управления информационной безопасностью (SIEM), которые управляют рисками и осуществляют мониторинг угроз для выявления подозрительной активности в сети.

Физическая защита охватывает много факторов, как внешних – например, нежелательное проникновение в ЦОД неавторизованных лиц, так и внутренних – негативное воздействие на оборудование внутри ЦОДа.

Наиболее надежная физическая защита ЦОДа – многоуровневая, с несколькими периметрами безопасности. Чем больше уровней – тем более защищенным считается объект. Базовый уровень предполагает наличие круглосуточной охраны и охраняемого внешнего периметра (забора). Внутри объекта показателем качественной защиты являются там-

ПРИМЕР ТЕХНИЧЕСКОГО ЗАДАНИЯ

Размещение (количество необходимых стойко-мест тех или иных габаритов):
Аренда стойко-места под стойку с габаритами 600 x 1070 мм 48U (1 шт.)
Аренда стойко-места под стойку с габаритами 600 x 1100 мм 48U (2 шт.)
Аренда стойко-места под стойку с габаритами 600 x 1200 мм 48U (1 шт.)
Аренда стойко-места под стойку с габаритами 1100 x 1200 мм 48U (1 шт.)

Внешние каналы связи (операторы связи, требования к каналам):
Оператор 1 – гарантированный канал 100 Мбит/с с выделенным маршрутизируемым «белым» IP-адресом с оборудованием оператора либо исполнителя.
Оператор 2 – гарантированный канал 100 Мбит/с с выделенным маршрутизируемым «белым» IP-адресом с оборудованием оператора либо исполнителя.
Оператор 3 – гарантированная возможность подключения «темного» оптоволокна.

Инсталляционные услуги:
1. Монтаж стойки и комплекта PDU на стойко-месте под ключ.
2. Подготовка инженерной инфраструктуры стойко-места для размещения стоек с подведением необходимого электропитания и лотками для коммутации.

Электропитание (требования по нагрузке и электропитанию):
1. К каждому стойко-месту подводится два независимых луча питания, каждый на свою группу PDU. Все PDU предоставляет ЦОД согласно тарифам.
2. Все стойки поддерживают нагрузку до 20 кВт с возможностью использовать тарифный план для стоек на 5 кВт.
3. АВР в аренду (3 шт.).

Дополнительные требования:
1. Фиксированные цены на предоставление стойко-места и электроэнергии.
2. Услуга «умные руки».
3. ЗИП-ячейка для хранения запчастей для «горячей» замены.
4. Все передаточные документы должны передаваться в электронном виде через систему ЭДО.

бур-шлюзы, датчики движения, круглосуточное видеонаблюдение, а также интеллектуальные системы контроля доступа с использованием биометрических технологий. Чем мощнее биометрическая защита, тем выше уровень надежности дата-центра.

Серьезную угрозу безопасности и бесперебойной работе ЦОДа создает неправильный температурный режим. Для устранения этого фактора риска применяются современные системы охлаждения, вентиляции и электропитания, а также системы мониторинга ЦОДа, которые позволяют получать информацию о нештатных ситуациях (возгорание, протечка, задымление). В случае фиксации задымления обязательно должна активироваться система пожаротушения.

Непременно поинтересуйтесь, какие инженерные системы энергоснабжения, охлаждения и пожаротушения установлены в дата-центре, насколько эти технологии современны, каковы регламент и скорость реакции на аварию и ее устранение, а также как организован доступ в машзалы.

Вопрос 7. Насколько оперативно вы хотите провести инсталляцию в ЦОДе? Нужны ли вам склад и круглосуточный доступ на площадку? Как быстро техподдержка должна реагировать на ваши запросы? Говорит ли персонал по-английски?

Эти и многие другие вопросы относятся к уровню сервиса коммерческого ЦОДа, который определяется количеством инженеров, списком предлагаемых услуг, скоростью реакции на запросы клиентов (декларируемой и реальной) и другими параметрами. Например, на всех площадках IXcellerate время отклика на обращения клиентов составляет, согласно SLA, 30 мин, но фактически не превышает 10 мин, а услуги удаленной техподдержки (remote hands) оказываются круглосуточно.

Для многих компаний важно иметь возможность работать с собственным оборудованием в любое время дня и ночи, а некоторые даже предпочитают арендовать офис и/или организовать склад на территории ЦОДа. Безусловный плюс при выборе ЦОДа – наличие специалистов, которым можно делегировать работу с оборудованием: администрирование, модернизацию, монтаж и демонтаж, настройку, тестирование, устранение неисправностей и т.д.

Набор и качество услуг, предлагаемых в разных дата-центрах, могут различаться. Составьте список услуг, которые требуются вам, и поинтересуйтесь их наличием у потенциального провайдера.

Вопрос 8. Комфортно ли вам общаться с представителями ЦОДа? Насколько они готовы прислушиваться к вашим требованиям и идти на уступки?

Цифры цифрами, технологии технологиями, но человеческий фактор пока никто не отменял. Каждому потенциальному клиенту ЦОДа важно лично приехать посмотреть на объект – но не только для того, чтобы заглянуть в технические документы, убедиться, что декларации соответствуют фактам, и своими глазами увидеть, как все организовано. Личное впечатление о людях – сотрудниках дата-центра – может сыграть решающую роль.

Опыт управленческого персонала, квалификация специалистов, отвечающих за надежность работы инженерной инфраструктуры, имеют огромное значение, но дело не только в профессионализме. С этими людьми вам предстоит работать достаточно долгое время, и желательно иметь уверенность в том, что с ними вам будет комфортно взаимодействовать.

Насколько гибко представители ЦОДа подходят к запрашиваемым условиям размещения? Насколько терпеливо и внимательно отнесутся ко всем вашим требованиям и запросам? Есть ли внутри объекта специальные комнаты для работы и отдыха клиентов? Готовы ли службы ЦОДа принять оборудование нестандартных размеров? Ответы на эти и другие вопросы помогут вам оценить уровень клиентоориентированности потенциального партнера еще до подписания договора.

Вопрос 9. Какова репутация потенциального партнера?

Репутация – неотъемлемый «ингредиент» правильно выбранного ЦОДа. На какие факторы стоит обратить внимание?

- Время присутствия компании на рынке свидетельствует не только о стабильности ее бизнеса, но и об опыте в предоставлении услуг.
- Динамика и стратегия роста: если компания все время развивается, строит новые объекты и имеет планы дальнейшего расширения своей экосистемы, это хороший знак.
- Финансовая прозрачность и стабильность: кто вкладывает деньги в компанию, какова репутация основателей и инвесторов, есть ли в открытом доступе бизнес-показатели?
- Клиентская база: с какими клиентами работает ЦОД, какие компании ему доверяют?
- Наличие сертификатов: Tier, ISO, PCI DSS и др. Сертификация – добровольная процедура, к которой прибегают не все компании, но она является объективным подтверждением того, что ЦОД соответствует всем необходимым стандартам. ИКС

Мы отвечаем за характеристики, которые заявляем

На рынок решений для ЦОДов выходит еще один амбициозный игрок – EKF. Как подчеркивает Алексей Чураков, руководитель направления «Телекоммуникационное оборудование TERACOM», бренд делает акцент на надежности поставляемых систем и их соответствии заявляемым характеристикам.

– EKF – новое имя для российских цодостроителей. Давайте познакомимся.

– За 21 год своего существования EKF прошел путь от локального сборщика щитовых изделий до крупного вендора электротехнического оборудования. Изначально мы ориентировались в основном на заказчиков из сегмента жилищного строительства. По мере развития компетенций EKF начал работать в более сложных сегментах рынка, например, выпускать решения для промышленной автоматизации, предложив в прошлом году реальную альтернативу продуктам ушедших вендоров.

Сегодня в портфеле EKF – более 17 тыс. артикулов продукции, порядка 400 товарных групп. Бренд располагает двумя крупными заводами во Владимирской области: в г. Александрове и п. Ставрово. Кроме того, мы используем другие производственные площадки в России, а также в Европе, Турции и Китае.

– С чем выходите на рынок ЦОДов?

– Мы решили начать с наиболее простых и понятных решений, предлагаемых в рамках линейки TERACOM: это СКС и кабеленесущие системы, шкафы, ИБП и PDU.

Производим медножильные СКС – в том числе потому, что есть пул традиционных заказчиков, которым «медь» интересна. Но, понимая, что в ЦОДах используется в основном оптика, запланировали развитие и этого направления. Сначала будем выпускать кабели, затем базовые оптические компоненты, укомплектованные кроссы и далее двигаться к полноценным претерминированным решениям, которые представим в следующем году.

По кабеленесущим системам у нас самая мощная в стране линия по производству перфорированных лотков. Также выпускаем лестничные, проволочные лотки, огнестойкие проходки. До конца года в портфеле появятся фальшполы. В следующем году – пластиковые лотки, спуски.

Производим широкий ассортимент телекоммуникационных шкафов. В ближайших планах – серверные шкафы, причем в комплекте с компонентами для формирования и изоляции коридоров (раздвижные двери, крыша и пр.).

– Что уже доступно в плане ИБП и PDU?

– Уже изготавливаем онлайновые моноблочные ИБП мощностью до 30 кВт. До конца года предложим источники мощностью до 200 кВт. Возможность установки их в параллель позволяет говорить о мегаваттных системах. Также в ближайших планах – модульные ИБП 25–200 кВт (силовые модули по 25 кВт) и 300–600 кВт (модули по 50 кВт). Все наши трехфазные ИБП поддерживают работу с литий-ионными АКБ.

В портфель PDU сначала вошли горизонтальные блоки для телекоммуникационных шкафов. Скоро представим вертикальные PDU, способные запитать больше оборудования в серверных стойках. Затем – полноценные управляемые PDU, которые не только распределяют питание, но и выдают его параметры и контролируют состояние рабочей среды в каждой стойке. Для таких PDU важно качественное ПО управления. Развитие софта – приоритетный вектор для EKF. До конца года запустим полноценную облачную SCADA-систему, в которой будет модуль управления PDU. Эта система позволит управлять всеми инженерными системами, установленными в ЦОДе.

– Где выпускаются ИБП и PDU?

– Сегодня мы используем контрактное производство в Китае. К выбору фабрик подошли самым тщательным образом. Продукты производятся в строгом соответствии с нашими требованиями. Большая команда EKF находится в Китае для контроля качества продукции, проверяем каждую партию, каждое изделие. Мы понимаем, что от надежности поставляемых решений и соответствия заявляемым характеристикам напрямую зависит наш успех у серьезных заказчиков, включая ЦОДы.

Сейчас в центральном офисе в Москве монтируем большой шоу-рум, где хотим представить не просто ассортимент продукции, а готовые решения для ЦОДов. Планируем построить небольшой коридор с системами бесперебойного питания, кабельными трассами, спусками, фальшполом, а в перспективе и с системой охлаждения.

Мы готовы идти навстречу заказчикам, разрабатывать интересные для них условия, формировать ЗИП, чтобы гарантировать непрерывность функционирования их объекта. При этом, повторю, особое внимание уделяем надежности нашей продукции, строгому соответствию заявленным техническим характеристикам, а также наращиванию наших профессиональных компетенций.

EKF
ekfgroup.com

Как заказать ЦОД под ключ

Коммерческий директор PNK group Евгений Скаридов рассказывает о том, как ускорить строительство столь необходимых сегодня ЦОДов, и о новых возможностях, которые девелопер предлагает их операторам.

– Еще в 2020 г. появилась информация о том, что PNK group планирует выходить на рынок ЦОДов. С тех пор и до сего времени игроки рынка задаются вопросом: какую нишу девелопер индустриальной недвижимости выбрал в этой, в целом новой для себя сфере?

– Во многих странах мира девелопмент ЦОДов – часть рынка индустриальной недвижимости. Поэтому неудивительно, что мы давно заинтересовались этим сегментом, изучали опыт разных стран. Приступив к развитию новой площадки в Москве на ул. Чермянской – она получила название PNK парк Медведково, – мы обнаружили, что эта промышленная территория с выделенными электрическими мощностями отлично подходит для ЦОДа. Соответственно на этом проекте мы и решили воплотить наши идеи по строительству ЦОДов и начали наращивать свои компетенции в данном направлении. В результате удалось создать два объекта по 4800 стойко-мест каждый. Нашим бизнесом всегда был и остается девелопмент. ЦОД – один из наших продуктов, который можно купить или взять в аренду.

– То есть вы не собираетесь становиться оператором ЦОДов и предлагать colocation и другие услуги на их основе?

– Мы планируем оказывать девелоперские услуги операторам ЦОДов – точно так же, как мы оказываем, например, услугу строительства завода, на котором клиент намеревается что-либо производить. Мы лишь построим завод, но производить на нем продукцию будем уже не мы. Так же, как и завод, оператор может приобрести ЦОД в собственность или взять в аренду.

– Что представляют собой два ваших ЦОДа в PNK парке Медведково?

– Эти два объекта имеют разные архитектурные концепции, но построены по схожим технологиям. Первый корпус – двухэтажный. Он изначально планировался как универсальное здание. Уже в процессе возведения было принято решение о его перепроектировании и создании в нем дата-центра. Оператором ЦОДа является «Ростелеком-ЦОД».

Второй корпус – шестиэтажный дата-центр. Оператор ЦОДа – сеть дата-центров 3data, которая запустила проект больших ЦОДов 3data HyperScale, рассчитанный на крупных заказчиков.

Каждый ЦОД общей электрической мощностью 36 МВт рассчитан на 4800 стоек при мощности стоек 5 кВт. ЦОД состоит из четырех модулей. Каждый модуль имеет два независимых ввода с напряжением 10 кВ, систему гарантированного питания, состоящую из шести ДГУ контейнерного исполнения (N + 1), и систему бесперебойного питания с резервированием 4/3N. В основе систем охлаждения – связка одного чиллера и двух прецизионных кондиционеров. На два машинных зала работают восемь таких холодильных систем. Резервирование – N +1. Оба ЦОДа оборудованы системами газового пожаротушения и раннего пожарообнаружения. Площадки имеют сертификат Uptime Institute на проект (Design), в ближайшее время планируем пройти сертификацию самих объектов (Facility).

– Таким образом, вы фактически передаете оператору полностью готовый к эксплуатации ЦОД?

– Совершенно верно. Оператору остается только расставить стойки в машинном зале и построить техническую СКС до предоставленных коммутационных кроссовых объектов. Оператор ЦОДа сам определяет провайдеров связи, которые на его объекте будут предоставлять телекоммуникационные услуги по каналам, построенным и переданным PNK group. Все спланировано для перспективы – по мере увеличения спроса оператор только устанавливает дополнительные стойки в машинном зале и оперативно масштабирует свой бизнес.

– Системы инженерной инфраструктуры у ЦОДа более сложные, чем у других типов индустриальных объектов. Какой экспертизой обладает PNK group?

– В процессе проектирования и возведения наших ЦОДов в PNK парке Медведково мы имели возможность привлекать многих российских и международных экспертов. Но главное, что эти проекты помогли нам создать собственную команду, обладающую необходимым опытом и

знаниями и продолжающую развиваться. В 2023 г. наши ведущие инженеры сертифицированы Uptime Institute.

Ничто так не демонстрирует экспертизу, как уже построенные, введенные в эксплуатацию и переданные в управление оператору объекты. Мы рады их показать, как виртуально, с помощью видеопрезентации, так и на реальной экскурсии.

– Как вы решаете вопросы комплектации объектов в условиях санкций и турбулентности на рынке?

– Все основные конструктивные элементы зданий PNK group производит на собственных заводах в Московском регионе. Это обеспечивает высокие качество и скорость возведения зданий.

Оборудование для ЦОДов в PNK парке Медведково мы приобретали и поставляли в 2022–2023 гг., и все обязательства нашими поставщиками выполнены. То есть вопрос комплектации оборудованием также решаем. На рынке идет процесс импортозамещения, на комплектацию будущих объектов он повлияет положительно. Имея опыт индустриального строительства, мы хорошо знаем рынок производителей и поставщиков энергетического, холодильного и прочего инженерного оборудования. Мы находимся в постоянном контакте с ними и видим, что они продолжают развивать свои продукты и сервис для клиентов из России.

– На рынке индустриального строительства PNK group возводит объекты гигантских площадей за несколько месяцев. Каковы перспективы сокращения сроков строительства ЦОДов?

– Вы правы, наша технология строительства дает возможность возводить объекты достаточно быстро, и это, безусловно, одно из наших ключевых преимуществ. В настоящий момент мы внедряем систему строительства ЦОДов, которая включает в себя использование предварительно изготовленных модулей здания и инженерного оборудования. Модульная система позволит создавать ЦОД под ключ менее чем за год. Также немаловажно, что финансирование наших объектов происходит за счет средств инвестиционного фонда, входящего в PNK group. Это дает возможность создавать складские запасы оборудования, имеющего длинные сроки поставки, что важно и при эксплуатации ЦОДов.

– PNK group предлагает свои объекты как для покупки, так и в аренду. Сама схема сдачи ЦОДа в аренду не очень распространена на российском рынке. Могут ли клиенты чувствовать себя защищенными от того, что владелец объекта расторгнет договор аренды с оператором?

– На рынке индустриальной недвижимости, к которому относятся и центры обработки данных, приняты долгосрочные контракты, защищенные от расторжения для обеих сторон. Также договор не может быть расторгнут либо изменены какие-либо его условия при смене собственника объекта недвижимости. Как правило, владельцами ЦОДов, сдаваемых в аренду, являются инвестиционные фонды, ориентированные на получение арендного потока. Для них договор аренды, скажем, на 10 лет, с оператором ЦОДа – большое преимущество, так как обеспечивает устойчивый

арендный поток. Поэтому клиенты ЦОДа, оператор которого арендует объект у инвестиционного фонда, могут чувствовать себя в такой же безопасности, как если бы оператор ЦОДа был его владельцем.

– Каковы ваши дальнейшие планы?

– У нас несколько перспективных площадок под ЦОДы в Москве, Санкт-Петербурге, Екатеринбурге и Новосибирске. Мы открыты к диалогу со всеми операторами дата-центров по реализации для них проектов в этих локациях.

«Пазл» СБГП складывается: от аккумуляторов до дизель-генераторов

Александр Барсков

В области систем бесперебойного и гарантированного электропитания ЦОДов процесс замещения ушедших брендов завершается. Новые вендор-листы формируются из российских и китайских производителей.

Система электроснабжения ЦОДа состоит из множества подсистем и компонентов (рис. 1). Но для заказчиков ключевыми ее элементами, несомненно, являются источники бесперебойного питания (ИБП), а также их неотъемлемый элемент – накопители энергии в виде аккумуляторных батарей. Именно эти элементы оказались в фокусе внимания на прошедшей в мае конференции DCDE-2023.

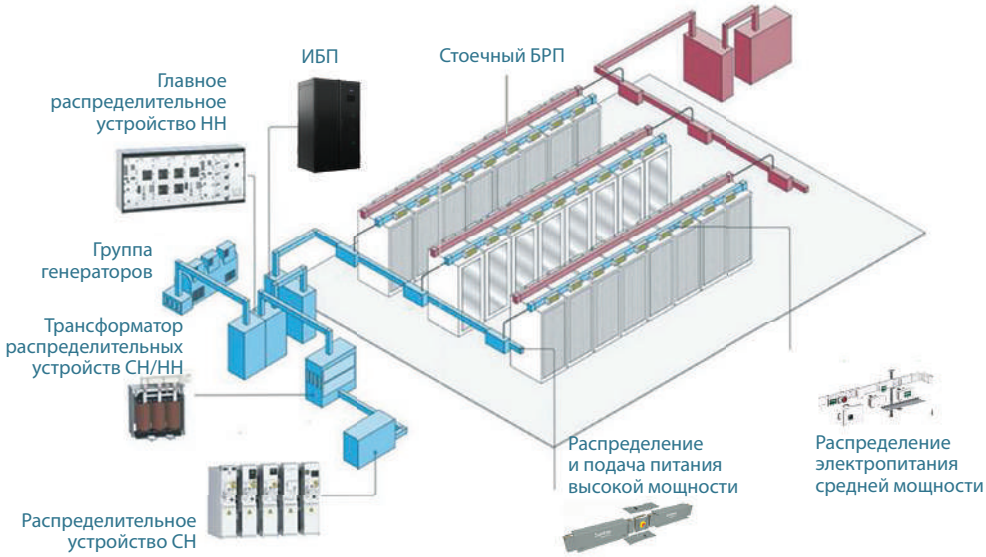
Как выбрать аккумулятор

По данным Uptime Institute за 2022 г., большая часть отказов ЦОДов (44%) связана с работой системы электроснабжения. В свою очередь, в этой системе самым слабым звеном оказываются аккумуляторные батареи (АКБ) – из-за них происходит 40% отказов в случаях проблем в системе электроснабжения. Из этой статистики ясно, что аккумуляторы – ключевой элемент, определяющий надежность работы ЦОДа. Однако, как сетует Александр Беспалов, руководитель отдела управления продукцией компании ENERGON (поставляющей АКБ под брендом Delta), выбору АКБ заказчики не всегда уделяют должное внимание.

По словам эксперта ENERGON, покупатели, как правило, интересуются параметрами первого уровня (рис. 2) – разрядными характеристиками, сроком службы, саморазрядом, весом, – которые у всех поставщиков более или менее одинаковы. Но это только верхушка айсберга, определяющего качество и надежность функционирования АКБ.

Второй уровень от большинства заказчиков обычно скрыт. Особенности химических процессов и добавки, количество пластин, их масса и геометрия, толщина сепараторов, технология производства – все это сильно влияет на срок службы, качество и потребительские характеристики. Например, для ЦОДов ENERGON предлагает высокоразрядные АКБ Delta Expert. В них больше электродов в сравнении со стандартной серией, а значит, увеличивается активная площадь, что позволяет отдать больше тока в единицу времени. Хотя внешне эти АКБ похожи на другие аккумуляторы Delta, но компоновка элементов совсем другая и даже при меньшей емкости разница в отдаче мощности существенная.

До третьего же уровня при выборе АКБ не добирается почти никто. Это особенности произ-



- ТП / Ввод от подключения к общей сети
- Трансформатор
- Главный распределительный щит (ГРЩ)
- Автоматический ввод резерва (АВР)
- Дизель-генераторная установка (ДГУ)
- Шинопровод
- Источник бесперебойного питания (ИБП)
- Распределительный щит бесперебойного питания (РЩБП)
- НКУ групп стоек
- Стоечный БРП (PDU)

Источник: Systeme Electric

Рис. 1. Основные элементы системы электроснабжения ЦОДа ▼

УРОВЕНЬ 1
Характеристики продукта

- Разрядные характеристики
- Срок службы
- Саморазряд
- Вес
- Бренд

УРОВЕНЬ 2
Неявные характеристики и содержимое продукта

- Максимальный ток КЗ
- Максимальный разрядный ток
- Химия и добавки
- Количество пластин, их масса и геометрия
- Толщина сепаратора

УРОВЕНЬ 3
Особенности производителя и поставщика

- **Качество техпроцесса** производителя
- **Стабильность характеристик** разных партий
- Количество и качество **точек контроля качества АКБ** (наличие мощностей, методологии и специалистов, процесса тестирования)
- Обслуживание АКБ в **логистической цепочке**
- Регулярная **работа над продуктом** – применение производителем обратной связи по поводу характеристик и качества
- **Складское наличие** для обеспечения срочной потребности и долгосрочный резерв для обеспечения успеха проекта
- **Техническая экспертиза** и пресейл, расчет наилучшего технического решения под каждое конкретное применение

Источник: ENERGON

▲Рис. 2. Характеристики, которые следует учитывать при выборе АКБ

водителя и поставщика – качество техпроцесса, стабильность характеристик разных партий, количество и качество точек контроля качества АКБ, обслуживание АКБ в логистической цепочке и пр.

Понятно, что для надежного эффективного функционирования любой системы важно ее профессиональное обслуживание. Чтобы АКБ были гарантированно заряжены и обеспечивали необходимый (расчетный) резерв времени для запуска ДГУ, А. Беспалов советует регулярно (раз в квартал) проверять их состояние – измерять температуру и напряжение. Раз в полгода рекомендуется проводить контрольно-тренировочный цикл, позволяющий оценить разрушение сульфата, скорректировать время автономии, устранить разбалансировку и обнаружить неисправные АКБ.

Помочь в обслуживании АКБ может специальная система мониторинга. Такую систему (DEMS) разработала и предлагает компания ENERGON. Она измеряет ток в цепи, температуру и напряжение каждой АКБ. На основе анализа собранных данных DEMS рассчитывает оставшийся срок службы АКБ с учетом условий эксплуатации и дает рекомендации для его продления. По данным, которые привел А. Беспалов, только за счет экономии ФОТ система может окупиться за 12 мес. Ну а повышение надежности и исключение аварий переоценить трудно.

Этот непредсказуемый литий

Вопроса выбора технологий АКБ представитель ENERGON не касался. Понятно, что большая часть поставляемых в ЦОДы аккумуляторов, в том числе продуктов ENERGON, – это свинцово-кислотные батареи (хотя у этой компании есть и литий-ионные АКБ – соответствующее производство было открыто в прошлом году в Турции). Но отношение заказчиков к этой технологии за последний год стало более прохладным. И дело не только и даже не столько в кратном повышении стоимости литиевого сырья (цена АКБ при этом выросла лишь на 25–30%), сколько в уходе с рынка основной движущей силы ЛИ АКБ – таких компаний, как Schneider Electric и Vertiv.

Однако появились новые адепты лития, в первую очередь компания РЭНЕРА, входящая в корпорацию «Росатом». Как рассказал Алексей Нешта, руководитель направления «Энергетика» этой компании, все началось с приобретения зарубежного предприятия полного цикла – небольшого, выпускающего аккумуляторы суммарной емкостью 150 МВт·ч в год, но с мощным подразделением R&D. Соответственно в России в 2021 г. было создано небольшое сборочное производство (всего на 15 МВт·ч), которое занималось ознакомлением с литий-ионной технологией и старалось интегрировать ее в различные решения. В прошлом году производственные мощности этого предприятия увеличились до 150 МВт·ч, в нынешнем увеличатся еще вдвое. В Калининграде строится гигафабрика (уже на 4 ГВт·ч), которая начнет работать в 2025 г. «Но и этого объема будет явно недостаточно для рынка, особенно с учетом перспектив развития электротранспорта. Поэтому мы рассматриваем площадки для следующих очередей», – поделился планами А. Нешта.

Как подчеркнул представитель РЭНЕРА, важно, особенно в нынешних условиях, что все патенты зарегистрированы в РФ, компания владеет технологией и сейчас ее локализует в России. Сегодня базовый продукт – литий-ионные ячейки четвертого поколения (Gen 4) для электротранспорта и систем накопления электроэнергии (рис. 3). Ячейки собираются в модуль, а из модулей строится готовое решение, например батарейный шкаф,

который интегрируется с ИБП. К концу года в производство будет запущена ячейка нового поколения с большей объемной энергоемкостью. Именно эти ячейки (VDA) будут производиться на гигафабрике в Калининграде.

На вопрос о пожароопасности ЛИ АКБ А. Нешта ответил, что безопасность обеспечивается на нескольких уровнях. На уровне ячейки применяются керамический сепаратор и другие средства, которые гарантируют отсутствие критического нагревания даже при физическом разрушении, что подтверждено соответствующими тестами. Кроме того, используется трехуровневая (на уровне ячейки, модуля, шкафа) система управления BMS, которая контролирует все важные параметры и, если какой-либо параметр выходит за установленные пределы, просто отключает аккумулятор. «Никакого возгорания произойти не может. Опасность представляет только внешний пожар, который может привести к возгоранию лития», – уверен эксперт РЭНЕРА.

Компания уже интегрировала свои АКБ и ИБП ряда производителей. «Когда и BMS, и все ПО принадлежит нам, интегрироваться с ИБП любого производителя достаточно просто», – отметил А. Нешта.

Ставка на модули

Что касается архитектуры ИБП для ЦОДов, то, похоже, побеждает модульность. По крайней мере на DCDE-2023 все производители ИБП делали акцент именно на модульных своих продуктах. Говоря о преимуществах модульных архитектур, Алексей Морозов, руководитель отдела маркетинга компании «Парус электро», выделил резервирование основных элементов системы (повышение отказоустойчивости), минимальное время обслуживания благодаря «горячей» замене модулей, а также простое масштабирование системы путем добавления силовых модулей и кабинетов.

В линейке «Парус электро» присутствует несколько модульных серий ИБП. Для небольших ЦОДов компания предлагает решение на базе силовых модулей по 20 кВт (высотой 2U) – в один кабинет устанавливается до 10 таких модулей, в параллельную систему – до четырех кабинетов. Для более крупных объектов выпускаются решения на базе модулей 50 кВт (3U) – кабинеты до 1 МВА с параллельной работой до шести кабинетов. Наконец, новая линейка – для крупных ЦОДов с высокими требованиями к плотности мощности – строится на модулях 100 кВт. При этом высота модулей остается равной 3U – за счет применения современных компонентов на основе карбида кремния, как объяснил А. Морозов. Уже доступны кабинеты на 400, 500 и 600 кВА; в этом году появятся кабинеты до 1,6 МВА. В параллельную систему можно объединить до восьми кабинетов.

Даже ИБП, которые формально относятся к моноблочным, внутри – модульные. Пример такого решения представила компания Ippon. Innova RT II 33 – трехфазный моноблочный ИБП (70–210 кВт, до 840 кВт в параллельной системе) с модульной архитектурой. «Заказав фрейм, можно установить (в него) один модуль на 75 кВт. При увеличении нагрузки можно добавить модули, но не в “горячем” режиме. Модульность помогает в обслуживании, позволяет унифицировать модельный ряд и ЗИП. Можно изъять необходимый модуль и провести с ним работу», – объяснил Алексей Лобов, директор по развитию бизнеса трехфазных ИБП компании Ippon. По сути, главное отличие такого ИБП от настоящего модульного – отсутствие возможности «горячей» замены модулей (рис. 4).

В портфеле компании, лидирующей на российском рынке ИБП как по числу проданных устройств, так и по объему продаж, есть и настоящий модульный аппарат. Innova Modular (75–200 кВт в одном шкафу, до 1,6 МВт в параллельной системе) построен на базе силовых модулей по 25 кВт. «Зарядный блок у каждого модуля на 25 А, это в среднем на 25–30% выше, чем у конкурентов. “Машину” на 200 кВт можно подключить к батарейному массиву с автономией более 3 ч. Установив второй ИБП, можно

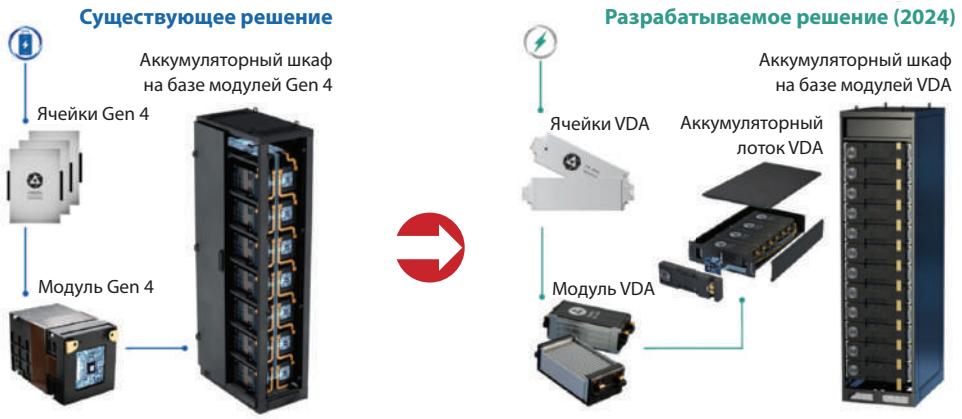


Рис. 3. ▶
Эволюция предложения компании РЭНЕРА

Источник: РЭНЕРА

получить резерв на 6 ч. Это важно там, где нет ДГУ», – говорит А. Лобов.

Недавно Ippon открыла в Москве технический центр, где можно подтвердить технические характеристики ИБП, заявленные в спецификации. Сегодня, в период смены вендор-листов, для ЦОДов это очень важно. Сервис на протяжении всего жизненного цикла обеспечивают 200 центров в России и СНГ. Ну и «вишенка на торте» – склад, на котором находится более 90 тыс. ИБП. Только трехфазных модульных ИБП – на несколько десятков мегаватт.

В 2023 г. модульные ИБП вывела на рынок и компания ДКС. Модель Trio MDA строится на основе силовых модулей по 25 кВт – мощность одного ИБП до 200 кВт, в параллельной системе может быть два таких ИБП. В модели Trio MDB используются силовые модули по 50 кВт, мощность одного устройства до 400 кВт, в параллель устанавливаются четыре ИБП.

В числе преимуществ модульных ИБП Александр Титов, менеджер по продукции ДКС, назвал режим «умного сна». Он позволяет задействовать только то число модулей, которое в данный момент необходимо для поддержки нагрузки с учетом резервирования. При повышении нагрузки спящие модули переходят в рабочий режим, причем у ИБП Trio MD модули «просыпаются» не более чем за 4 мс.

ИБП с двумя типами модулей предлагает и Systeme Electric. Устройства Excelente VL компонуются модулями по 50 кВА, а Excelente VX – 100 кВА; мощность одного ИБП в обоих случаях – до 600 кВА. Алексей Соловьев, технический директор управления по рынку «Информационные технологии», отмечает компактность ИБП (для VL ширина стойки 600 мм, для VX – 800 мм).

Systeme Electric с рекордной скоростью расширяет свой портфель решений для ЦОДов, по своему ассортименту уже приближающийся к тому предложению, которое было у Schneider Electric. По утверждению А. Соловьева, компания предлагает практически все основные компоненты системы энергоснабжения ЦОДа (за исключением ДГУ): от ячеек среднего напряжения, трансформаторов и ГРЩ до шинопроводов и PDU (см. рис. 1). Причем, рассказывая о новой продукции, представитель Systeme Electric подчеркивал, что поставщики основных комплектующих те же, что и у Schneider Electric, часть оборудования изготавливается на тех же производственных линиях, с применением тех же материалов и технологий.

Как и Schneider Electric, Systeme Electric делает ставку на предложение заказчикам комплексного инфраструктурного решения. «Это комплексная ответственность, понимание всех смежных вопросов, комплексная сервисная поддержка, это заранее проделанная интеграция всех систем, наконец, это унификация ЗИП для службы эксплуатации (не надо мучиться с “зоопарком”)», – перечисляет преимущества такого подхода А. Соловьев.

Источник: Ippon

▲ Рис. 4. Моноблочный ИБП с модульной архитектурой Innova RT II 33 и модульный Innova Modular

Что же касается ДГУ, то, как известно, девятый и десятый пакеты санкций практически остановили поставки генерирующего оборудования западных компаний, традиционно использовавшегося российскими производителями ДГУ. Компания «НГ-Энерго» переориентировалась на двигатели китайской Yuchai. Как рассказал Андрей Зотиков, директор по продажам направления «Инфраструктура» компании «НГ-Энерго», Yuchai – лидер среди производителей промышленных двигателей в Китае с годовой производственной мощностью более 800 тыс. двигателей. Важно, что двигатель – собственная разработка Yuchai, и все основные комплектующие изготавливаются на заводах этой компании.

Электростанции для ЦОДов «НГ-Энерго» строит на основе 16-цилиндрового V-образного двигателя объемом 105 л. Как отмечает эксперт «НГ-Энерго», время пуска ДГУ из прогретого состояния не более 15 с, а единовременный прием нагрузки – до 85% номинальной мощности без аварийной остановки агрегата. Все электростанции на базе двигателей Yuchai комплектуются панелью управления «Овен». Соответствующее ПО – собственная разработка «НГ-Энерго». По данным компании, в ЦОДах уже инсталлированы ДГУ на базе двигателей Yuchai общей мощностью 70 МВт.

Таким образом, все фрагменты пазла под названием «полное решение для системы бесперебойного и гарантированного электропитания ЦОДа» занимают свои места. Да, на новых компонентах, для окончательной проверки которых требуется время. Но тщательное предварительное тестирование, проведенное ответственными производителями, внушает оптимизм. ИКС

ДКС: здесь и сейчас

Последовательно расширяя портфель продуктов для ЦОДов, компания ДКС стала ведущим российским производителем в этом сегменте и намерена к 2025 г. занять 25% рынка. На вопросы «ИКС-Медиа» отвечает Денис Горяченков, руководитель отдела телекоммуникационных проектов компании.

– Несколько лет назад ДКС объявила о планах стать производителем полного комплекса решений для инженерной инфраструктуры ЦОДов. Как продвигается воплощение этих планов в жизнь?

– Развиваем текущие продуктовые линейки, выводим на рынок новые. Например, в 2022 г. выпустили оптические претерминированные решения, системы изоляции коридоров, низковольтные комплектные устройства. Недавно объявили о выводе на рынок модульных ИБП с мощностью одного устройства до 400 кВт. В области комплексного предложения для ЦОДов оборудования электроснабжения и слаботочных систем мы сегодня самые крупные производители в России.

– Но в вашем портфеле пока отсутствуют системы охлаждения. Насколько это является проблемой?

– Не считаю это проблемой. Всему свое время. Системы охлаждения могут у нас появиться, но тогда, когда компания обретет соответствующие компетенции, научится их производить самостоятельно. А просто поставлять оборудование из Азии нам неинтересно. Это не наша философия.

Скажу больше. У ДКС, компании с оборотом около 50 млрд руб. и сотней различных продуктов, нет собственных PDU, хотя о них спрашивает чуть ли не каждый заказчик. Конечно, можно покупать PDU в Китае, брендировать торговой маркой ДКС и продавать через нашу партнерскую сеть, рассказывая всем, какой это замечательный продукт. Но мы – ПРОИЗВОДИТЕЛЬ. Почти все, что надо для PDU (розетки и пр.), мы уже выпускаем на своих заводах. Не хватает программного обеспечения. До конца года завершим его разработку, представим собственную систему мониторинга и управления. Тогда и выпустим PDU. И они будут опробованы нами и протестированы заказчиками.

– Но в России, как грибы после дождя, появляются компании, предлагающие «почти все», что надо ЦОДам. Не проиграете ли им в конкурентной борьбе?

– Да, сейчас немало компаний, которые мнят себя крупными производителями, но на деле оказываются просто дистрибьюторами китайских товаров. На рынок выплескивается много некачественных, откровенно «сырых», неадаптированных к требованиям российских заказчиков продуктов. Это только размывает преимущества «комплексных решений». Да и смогут ли российские псевдопроизводители, которые заявляют, что у них есть все, обеспечить должное обслуживание, поддерживать это оборудование в гарантийный и постгарантийный периоды?

– Действительно, проблема «сырых» продуктов сейчас стоит остро. Но кто не ошибается?

– В этом вы правы. Вопрос в работе над ошибками. Помню историю, когда в одном крупном ЦОДе «вылетела» половина кондиционеров именитого западного бренда. Компания признала, что это заводской брак, и оперативно все исправила. И заказчик продолжил с ней сотрудничать.

Нам тоже аукается один цодовский проект. Там «накосячили» все: и проектировщики, и монтажники, и мы – для нас это был первый проект такого рода. Но ДКС взяла на себя дополнительные обязательства и поменяла часть оборудования. И наше оборудование работает, ЦОД работает. А это главное.

Ошибки бывают у всех. Но мы их признаем и исправляем. А не исчезаем и не меняем юрлицо, как некоторые.

– Как вы работаете с крупными ЦОДами?

– Если раньше «на фронте стоял сейл», в крайнем случае менеджер по ключевым клиентам, то сейчас ситуация изменилась. На первом месте от нас выступают технические специалисты, главные инженеры проектов. Регулярно, раз в неделю, а то и чаще, проводятся совещания с заказчиком. Зачастую приходится «подтягивать» его экспертизу. Вот недавний пример. Заказчик запрашивает лоток толщиной 1,2 мм. Нам выгодно продать такой лоток, он дороже обычного, но мы спрашиваем: «Зачем?». Ответ: «Я в нефтянке работал, там такие прокладывали». Разъясняем: «Там нагрузки другие, снег лежал на лотке, а здесь все в здании».

В результате подбираем оптимальный вариант и экономим средства заказчика.

Та часть, которая у нас как у производителя отсутствует (те же PDU), обеспечивается продуктами других производителей с помощью дистрибьюторов. Мы же в предлагаемом комплексном решении выступаем как эксперты и отчасти как проектировщики – иногда приходится доделывать или переделывать проекты.

– Насколько знаю, ИБП для ЦОДов вы производите на своем заводе в Италии. Возникают ли сложности с доставкой?

– Да, моноблочные ИБП делаем в Италии. Пока санкции не препятствуют поставкам. Скоро анонсируем ИБП нового поколения – на 60 и 100 кВА. Элементная база нового поколения. В России такая просто недоступна.

А вот модульные ИБП, которые анонсировали на конференции DCDE-2023, изготавливаем на контрактном производстве в Китае. К поиску площадки для производства таких ИБП приступили еще три года назад. Все решения тщательно протестировали, подписали долгосрочный эксклюзивный договор. Мы единственные в России, кто работает с этим заводом.

– Давайте поговорим о сервисе. Западные вендоры приучили к высокому уровню, начиная с проектирования: BIM-модели оборудования и пр. Насколько ДКС соответствует лучшим мировым практикам?

– Если уж речь зашла о BIM, то ДКС здесь стояла, что называется, у истоков. Мы одни из первых начали делать BIM-модели, еще в 2017 г. Сейчас модели есть на всю линейку продукции – может быть, исключая стяжки и другие простейшие изделия. Более того, внутри компании мы тоже используем BIM. Когда продуктовый маркетинг заказывает у коммуникационного маркетинга брошюры или каталоги, согласно внутренним процедурам, он должен предоставить BIM-модель. Все наши BIM-модели находятся в открытом доступе. Этим пользуются и наши партнеры, и наши конкуренты – берут и переделывают под себя. Но мы не против, ошибок при проектировании будет меньше.

Кроме того, мы предоставляем полноценную регистрацию проектов, и не в Excel или где-то в телефоне, а в серьезной CRM-системе. Ранее использовали систему SAP, но после ухода этой компании оперативно нашли замену в виде BPMSoft. Уже перешли на новую CRM-систему, причем ни заказчики, ни дистрибьюторы этого не почувствовали. Вся миграция заняла два дня, выходные. Все данные перенесли, ничего не потеряли, все сервисы работают.

Следующий этап – собственно поставка оборудования. Мы – одна из немногих компаний, которая не гонится за авансами, зато готова софинансировать крупные проекты. На старте проекта обсуждаем с заказчиком и с интегратором, что мы можем предложить, какие отсрочки платежа, какие банковские гарантии. Когда проект стоит миллиарды рублей, это важно.

Очень важно обучение персонала заказчика. Мы полноценно обучаем, как выполнять пусконаладку оборудования, как его эксплуатировать. Всегда есть нюансы. Как пример – наш шинопровод. ПУЭ требуют ежегодную протяжку болтовых соединений. Но наш шинопровод, если токи не превышают предельных значений, в этом не нуждается – достаточно визуального и теплового контроля.

– Для ЦОДов важна возможность оперативного решения проблем, замены отказавшего оборудования. Какие здесь есть возможности?

– Сейчас мы в партнерстве с несколькими крупными системными интеграторами разрабатываем сервисные SLA. До конца III квартала этот вопрос будет решен. Будет поддержка 24×7, быстрое реагирование, выезд инженера в течение 4 ч – все, к чему привыкли серьезные заказчики.

Кстати, на конференции DCDE-2023 обсуждали сервисное обслуживание оборудования ДКС с рядом команд ушедших вендоров. Их компетенции плюс наше оборудование – новая перспективная модель.

Мы не тянем весь сервис на себя. Обучаем партнеров и интеграторов, чтобы они могли выполнять пусконаладку наших ИБП, шинопроводов и другого оборудования, ставить его на гарантию. Гарантийный срок в зависимости от типа продукта – до четырех лет.

– Привели ли новые условия к каким-либо изменениям в выборе технологий? Нет ли отката, технологической деградации?

– По кабельным системам, СКС, ИБП все без изменений. Ячейки среднего напряжения у нас (у ДКС и еще ряда российских компаний) – на лучшем мировом уровне. (Некоторые так называемые российские производители повезли такие ячейки из Китая, завлекая ценой, – вот это точно шаг назад.) С трансформаторами тоже порядок. Сейчас по очень жестким требованиям одной из крупнейших ИТ-компаний готовим новые трансформаторы – такие выпускают только два завода в мире.

Но по АВР немного откатились назад. Последнее поколение автоматов с электронными расцепителями, которые умеют сами себя тестировать и контролировать, в РФ недоступно. В целом с системами автоматизации есть определенные проблемы. Дефицит контроллеров. И пандемия внесла свой вклад, и текущие санкции. Но все решаемо.

– И в конце разговора – о планах.

– ДКС продолжает инвестировать в строительство новых и развитие существующих фабрик в России. Уже в этом году мы анонсируем и откроем ряд новых площадок, выводящих нас на новые уровни.

Мы не меняем принципы и цели, сформулированные нашими основателями и акционерами. Одна из целей – к 2025 г. занять лидирующую (25%) долю на ИТ-рынке, в первую очередь на рынке ЦОДов. Мы планомерно, шаг за шагом движемся к достижению этой цели.

DCIM: учет и планирование в ЦОДе

Ключевые ресурсы любого ЦОДа: площадь, электроэнергия, холод и люди. Учет и планирование этих ресурсов сегодня важны как никогда. И с этой задачей успешно справляются системы класса DCIM.

Евгений Кривоносов, генеральный директор, «СДИ Софт»

Сергей Довгань, технический директор, «СДИ Софт»

«ИКС»: Что понимается под DCIM? Каковы основные назначение и функционал таких систем?

Сергей Довгань: DCIM (Data Center Infrastructure Management) дословно переводится как управление инфраструктурой ЦОДа. Но функционал таких решений сильно зависит от особенностей поставщика, его предыстории. Одни производители начинали с кабельного учета и потом, расширив функционал соответствующей системы, позиционировали ее как DCIM. Другие предлагают DCIM как развитие своей системы SCADA, третьи ведут свою историю от систем технического учета в ИТ и т.д.

Важнее то, чего ждут от DCIM заказчики, прежде всего службы эксплуатации ЦОДов. Под управлением инфраструктурой они понимают три основные задачи: учет и планирование ресурсов, мониторинг, а также управление работами, связанными с эксплуатацией и обслуживанием. DCIM в первую очередь решают именно задачи учета и планирования, позволяя контролировать все объекты эксплуатации, связи между ними, области ответственности.

Наши заказчики – это крупные ЦОДы. На таких объектах для названных функций – учета ресурсов, мониторинга и управления работами – используются специализированные инструменты. Например, система класса Service Desk для управления работами, SCADA – для мониторинга. Важно обеспечить интеграцию, скажем, системы мониторинга с системой DCIM. Последняя поставляет системе мониторинга информацию, показывая, где что должно находиться, как подключаться, как должен осуществляться мониторинг и т.д.

«ИКС»: Какие системы обычно находятся под управлением DCIM?

С.Д.: В коммерческих ЦОДах системы DCIM работают в основном с инженерной инфраструктурой. В корпоративных дата-центрах помимо этого часто с помощью DCIM ведут учет ИТ-оборудования, установленного в стойках, вплоть до отдельных плат, СКС, виртуальных серверов и их ресурсов, IP-адресного пространства и других логических объектов.

Кроме того, в корпоративных ЦОДах часто ставится задача интеграции с различными ИТ-системами, например, с базой данных управления конфигурацией (CMDB). В привычный для ИТ-специалистов контур управления инженерные системы обычно не входят. Более того, айтишники просто не замечают наличия таких систем, хотя без них никакие приложения работать не будут. DCIM позволяет расширить область управления для ИТ-подразделений, чтобы люди, отвечающие за функционирование прикладных систем, понимали влияние не только программных компонент, но и инженерной инфраструктуры ЦОДа. Ведь важно знать, от какого ИБП зависит работа ключевой ИТ-системы компании.

«ИКС»: Какова история появления и развития вашего ПО? Насколько оно независимо от зарубежных разработчиков?

Евгений Кривоносов: Изначально с 2010 г. мы сотрудничали с известным немецким производителем (FNT GmbH), одним из лидеров на рынке DCIM. Успешно продавали и внедряли его решение на рынках России и СНГ. Постепенно мы вырастили команду программистов, которые активно включились в разработки. Дело дошло до того, что большая часть кода модуля DCIM стала создаваться именно в РФ. После событий 2014 г. ряд заказчиков попросили нас локализовать продукт. Трансфер технологий шел пять лет, с 2014-го по 2019 гг., причем нам был передан не только исходный код, но и все юридические права на технологии. Сегодня наш продукт, «СДИ Базис» – полностью отечественное программное решение, внесенное в единый реестр российского ПО.

«ИКС»: Существует мнение, что готовые системы DCIM не подходят заказчикам, поскольку в каждом ЦОДе своя специфика. Поэтому каждый ЦОД пишет систему управления «под себя». Что скажете на этот счет?

С.Д.: Напрашивается пример из 90-х, когда все писали собственные складские системы. Зачастую «на коленке». Видимо, у компаний много было ресурсов, чтобы самим писать программы, и не было продукта, способного удовлетворить большинство запросов. Но через два-три года время самописных систем прошло.

«ИКС»: Но в ЦОДах действительно много специфики. Часто говорят, что одинаковых ЦОДов не существует.

Е.К.: Здесь важно отметить, что мы предлагаем не только программный продукт, но и огромную библиотеку цифровых моделей. В ней описано более 75 тыс. моделей устройств, которые используются в ЦОДах, – в этом уникальность нашего решения. Написать саму программу – это полдела, а вот на создание такой библиотеки требуются огромные ресурсы. Ее за один год не напишешь. Наша библиотека собиралась 20 лет и постоянно пополняется,

в том числе моделями российских продуктов, которые сейчас выводятся на рынок.

Многие заказчики выбирают нас именно по причине зрелости продукта, которая позволяет не беспокоиться о необходимости существенной кастомизации. Коробочный продукт настолько проработан, что дает возможность решать большинство задач, встающих в ЦОДах.

«ИКС»: Насколько сложно добавлять в DCIM поддержку оборудования нового вендора? Например, цифровые модели для нового российского оборудования?

Е.К.: Для нас это не проблема. У нас выделенная группа занимается созданием цифровых моделей. Они могут быстро подготовить модели всего, что появляется на рынке и на площадках заказчиков.

«ИКС»: Еще один стереотип: DCIM – очень дорогое решение. Насколько это верно? Каковы типовые сроки окупаемости вашего ПО?

С.Д.: Опять же приведу пример из другой области. Каков срок окупаемости бухгалтерской системы? Такая система прямого дохода не приносит, но является необходимым элементом системы управления предприятием. Это важнейший источник управленческой информации.

Схожая ситуация с DCIM. Это система, поддерживающая принятие управленческих решений для процессов эксплуатации и планирования в ЦОДе. Многие руководители оценивают пользу от этой системы через уменьшение числа сбоев благодаря лучшей информированности персонала о ресурсах и объектах ЦОДа. У нас есть статистика, что DCIM позволяет на 25% ускорить разрешение инцидента. Кроме того, она дает возможность сократить время на предоставление типовых услуг. За счет четкого описания всех ресурсов и планов их потребления снижаются расходы на закупки.

Немало и тех владельцев ЦОДов, которые оценивают DCIM через призму повышения качества предоставления услуг, которое просто невозможно обеспечить без учета и планирования ресурсов. Также есть компании с очень крупными службами ИТ, для которых ключевой является задача автоматизации. А это и повышение надежности (минимизация влияния пресловутого человеческого фактора), и сокращение фонда оплаты труда, и масса других плюсов. Понятно, что автоматизация невозможна без такой системы учета, как наша.

Е.К.: Часто причина покупки нашей системы – необходимость оптимального использования и наращивания основных ресурсов: места, энергии, холода. Мы можем не только документировать текущее состояние, но и давать временную перспективу потребления ресурсов. Это позволяет вовремя принимать обоснованные управленческие решения о наращивании ресурсов, а не узнавать об их дефиците, когда заказчик уже привез новые серверы для установки в ЦОДе.

«ИКС»: Можете привести примеры проектов внедрения вашей системы?

Е.К.: Один из крупнейших российских сотовых операторов попросил нас помочь детально задокументировать несколько десятков площадок ЦОДов – от Калининграда до Хабаровска, всего более 7 тыс. стоек. Требовалось паспортизировать ЦОДы с учетом загрузки стоек оборудованием, разобраться со свободными местами в стойках, свободными портами, потреблением электричества. Проект предусматривает много задач по интеграции – с системами ITSM, SCADA, системой учета кабельных соединений.

Другой пример – крупная федеральная служба, у которой несколько ЦОДов, тысячи стоек. Очень скрупулезный заказчик, долго выбирал, рассматривал различные продукты. В проекте реализована большая глубина учета, вплоть до планок памяти в серверном оборудовании, интеграция со смежными системами.

Вот пример из Казахстана – один из крупнейших операторов ЦОДов и провайдеров облачных сервисов компания «Транстелеком». Все начиналось с учета инженерного оборудования и серверов в контейнерных ЦОДах. Затем в систему стали вносить все больше информации, связанной с ИТ. У компании богатый ИТ-ландшафт, поэтому в проекте реализована интеграция с различными системами, в том числе мониторинга.

«ИКС»: Текущая ситуация подстегивает интерес заказчиков к системам DCIM?

Е.К.: Да, потребность в таких решениях растет. Причин тому несколько. Основные ресурсы, используемые ЦОДами, становятся труднодоступными, а потому использовать их надо более рационально. Взять, например, инженерное оборудование. Сегодня желательно заранее понимать, какое оборудование потребуется в будущем, – ведь ждать тот же чиллер или ДГУ придется много месяцев. Ситуация с COVID подчеркнула хрупкость человеческих ресурсов. Когда доступ на объект затрудняется, наличие его цифрового паспорта абсолютно необходимо для удаленного обслуживания.

С.Д.: Кардинальная смена вендоров и повышение требований к надежности ЦОДов, происходящие на фоне сокращения расходов на эксплуатацию и усиления дефицита квалифицированных кадров, – все это ставит перед руководителями ЦОДов все более сложные задачи. Нужен эффективный инструмент по учету и планированию ресурсов. И наше решение «СДИ Базис» – как раз такой инструмент.

«ИКС»: Как вы оцениваете российский рынок систем DCIM? Ваши позиции на нем?

Е.К.: Немало компаний позиционируют себя как поставщики систем DCIM. А конкуренция – это всегда хорошо. Но считаю, что по глубине проработки, числу инсталляций, возможности обеспечения отказоустойчивости, масштабирования у нашего продукта нет конкурентов. В нем учтен опыт порядка 600 внедрений. Одно из них – в компании Digital Realty, которая управляет 150 тыс. стоек. Это в три раза больше, чем емкость всего российского рынка коммерческих ЦОДов. В России у нас несколько десятков проектов общей емкостью почти 20 тыс. стоек. И это немало!

Дата-центр для каждого

Николай Носов

Использование предварительно изготовленных и модульных ЦОДов поможет снизить риски, связанные с уходом с российского рынка известных зарубежных брендов, и увеличить оснащенность предприятий вычислительными мощностями, столь необходимыми для проектов цифровизации.

Серьезные вызовы, связанные с изменением геополитической обстановки, санкциями, уходом западных вендоров и нарушениями цепочек поставок, привели, как отмечалось на организованной «ИКС-Медиа» конференции DCDE-2023, к сильной кастомизации проектов. ЦОДы стали уникальными, штучными объектами, своего рода произведениями искусства. Мало кто может купить картину мастера – скорее для украшения дома используют копию или репродукцию. Далеко не каждая компания может позволить себе обратиться к способной создать ЦОД команде профессионалов, тем более развернуть лабораторию для тестирования совместимости инженерного оборудования от новых вендоров, не имеющих авторитета и долгой истории успеха. А дата-центры нужны всем.

Возможный выход из этой ситуации – использование модульных и prefab-ЦОДов, в которых большая часть проблем совместимости оборудования перекладывается на поставщика, создающего типовые решения высокой заводской готовности. Благодаря серийности производства он может разработать проект на профессиональном уровне, развернуть тестовую лабораторию и обеспечить высокое качество поставляемой продукции. А потом в рамках договора отвечать за решение в комплексе, включая узлы не известных конечному заказчику поставщиков.

В сборочном цехе ДАТАРК ▶

Все в контейнере

Prefab-ЦОД мало собрать и протестировать на заводе. Его еще требуется доставить на место. Стандартная единица для перевозки – морской контейнер, который легко доставляется не только морским, но и железнодорожным и автомобильным транспортом. С выпуска дата-центров в морском контейнере, в котором можно разместить до восьми стоек, начинали большинство вендоров prefab-ЦОДов. По числу инсталляций ЦОД в одном контейнере – наиболее популярный формат и сейчас. Но эксплуатировать оборудование в узком стандартном морском контейнере тяжело.

«Мы не используем стандартные морские контейнеры. Все решения ДАТАРК базируются на стандартизированном мобильном контейнерном модуле, разработанном нашими конструкторами и позволяющем реализовать практически любые задачи заказчика с точки зрения как масштаба, так и условий доставки и эксплуатации», – рассказал технический директор и основатель компании ДАТАРК Евгений Тропин.

На основе мобильного контейнерного модуля ДАТАРК создает модульные ЦОДы высокой заводской готовности: от двух до 12 стоек в одном модуле и более 12 стоек в многомодульной компоновке. Например, ЦОД на 20 стоек составляется из трех-четырех модулей, образующих единый закрытый объем с функциональными отсеками.

Под торговой маркой POWERARK компания производит энергетические модули, которые обеспечивают гарантированное и бесперебойное электроснабжение ЦОДа либо комплексов автоматизации и связи. Внутри модулей POWERARK могут размещаться: трансформаторная подстанция, системы распределения питания, системы бесперебойного питания, накопители энергии. Мощность одного модуля от 50 кВт до 1,5 МВт, автономность работы от 3 мин до 1 ч.

▲ ЦОД GreenMDC

В феврале 2023 г. компания вывела на рынок ЦОДов автоматизированную систему мониторинга и управления DATCHECK, к концу года планирует начать выпуск микроЦОДов DATARK, которые позволят заказчикам построить ИТ-инфраструктуру в любом помещении с минимальными капитальными затратами. Посмотрим, смогут ли эти решения заменить аналогичную продукцию ушедшей с российского рынка компании Rittal.

Выгоднее, чем капитальный

По оценкам генерального директора компании GreenMDC Федора Клименко, российский рынок prefab- и модульных ЦОДов растет на 30–50% в год. При этом меняется его структура. «Многие заказчики уже понимают, что предварительно изготовленный или модульный ЦОД – это не контейнер, а инфраструктура большего размера», – отметил Ф. Клименко.

Начиная с 2007 г. самым популярным вариантом в России были контейнерные ЦОДы на 1–8 стоек. С 2013-го на рынок вышли решения из нескольких блоков на 8–30 стоек (десятки инсталляций). В 2016 г. появились единичные инсталляции больших prefab-ЦОДов – от 30 до более сотни стоек. Два таких проекта GreenMDC завершила в 2023 г.

Рынок оценил преимущества предварительно изготовленных ЦОДов. По мнению эксперта, prefab-ЦОД проще выбрать – не надо искать проектировщиков, интеграторов, проводить конкурс. Производителей, реально выпускающих prefab-ЦОДы, немного, поэтому чтобы выбрать продукт, соответствующий требованиям компании, понадобится менее двух недель. Объем проектирования при использовании prefab-ЦОДа меньше на порядок. По сути надо разработать только генплан, проект на внешние сети и паспорт модульного ЦОДа как изделия (он позиционируется как оборудование). И согласовать с пожарной инспекцией – сделать проект пожарной сигнализации, системы пожаротушения и автоматической противопожарной защиты.

Prefab-ЦОД быстрее и проще строить. Разница в объеме проектирования и строительства сильно влияет на сроки проекта. На создание модульного ЦОДа на 100–300 стоек под ключ у GreenMDC уходит 7–8 месяцев, строительство же аналогичного капитального займет, по оценке Ф. Клименко, полтора-два года (есть компании, которые умеют укладываться в год. – *Прим. ред.*). Кроме того, строительство капитального ЦОДа – это «тонны исполнительной документации», а с prefab-ЦОДом таких сложностей нет.

Для капитального ЦОДа интегратор может предоставить комплексную эксплуатационную документацию, где ЦОД будет описан как комплекс. Но это дополнительная работа в отличие от prefab-ЦОДа, где такая документация входит в состав решения. Клиент получает не десятки инструкций по использованию отдельных устройств, а одну, на prefab-ЦОД в целом.

Модульный ЦОД обеспечивает гибкость при оформлении. Согласно градостроительному кодексу РФ, prefab-ЦОД не является капитальным строением, поэтому его можно оформить как оборудование с паспортом. Плюсы такого подхода: достаточно иметь паспорт изделия вместо большого количества отдельных проектов; проще взаимодействовать с Государственным архитектурно-строительным надзором; меньше вопросов у проверяющих организаций. Минус подхода – нельзя получить адрес; для этого как раз потребуется оформить prefab-ЦОД как капитальное строение.

ЦОД для д’Артаньяна

Средние модульные ЦОДы – магистральное направление для компании Sitronics. «Для Атоса это слишком много, для графа де Ла Фер – слишком мало, а для д’Артаньяна в самый раз», – описал подход компании цитатой из культовой книги Игорь Анисимов, директор департамента центров обработки данных компании Sitronics. Основа «ЦОДа для д’Артаньяна» – модульный ЦОД Sitronics на 30 стоек и 150 кВт

Макет модульного ЦОДа компании Sitronics ▶

ИТ-нагрузки, предназначенный для масштабирования в кластер до шести модулей. Наиболее дорогой первый модуль включает в себя помещение для диспетчеров.

Дизайн модулей выполнен в соответствии с требованиями Uptime Institute для уровня надежности Tier III. Компоненты резервируются по схеме 2N или 2N + 1, что снижает риски использования малоизвестных брендов.

Транспортные габариты и фитинги эквивалентны стандартному 40-футовому контейнеру типа high cube и не доставляют проблем при транспортировке. Контейнеры в высоту достраиваются цокольными модулями высотой 1 м, которые партиями по три штуки транспортируются отдельно. Стойки размещаются в два ряда, по 15 штук в каждом.

Габариты позволяют осуществлять транспортировку без конвоя. Такие дата-центры можно погрузить на трак и привезти на место установки. Другой вариант – сборка модулей из полуконтейнеров стандартного типа, а половинки транспортируются стандартными средствами.

В модульном ЦОДе Sitronics используется энергоэффективная система охлаждения на базе установок косвенного адиабатического охлаждения (климатическое исполнение от −45 до +41°C), опционально оснащаемая элементами фреонового охлаждения. Использование адиабатики – особенность решения компании, отличающая его от конкурентов.

Адиабатические установки используются и для больших модульных ЦОДов на 120–750 стоек, которые компания предлагает для городов-миллионников. При этом весь ЦОД может собираться из стандартных контейнеров. Или же можно построить быстровозводимое здание без сварных соединений и внутрь него установить готовые модули инженерных и машинных залов.

В модулях без внесения существенных изменений в конструкцию здания ЦОДа размещаются все типы ИТ-нагрузок, стойки OCP, стойки высотой 48U и стойки мощностью более 10 кВт. Меняются только высота цокольного и антресольного модулей. В комплект поставки входят два ДГУ (2N) в контейнерном исполнении с низким уровнем шума и запасом топлива на 12 ч автономной работы каждый.

Компания тщательно тестирует отечественные решения, за счет которых доля импортозамещенных изделий в модульном ЦОДе может достигать 70%. Дополнительное конкурентное преимущество – собственное ИТ-оборудование: серверы SIT SRH2221 V5 (№ 4521/1/2022 в реестре Минпромторга) и появившаяся в феврале 2023 г. в реестре отечественного ПО (№ 16518) своя платформа виртуализации.

«Компания предлагает комплексное решение ”ЦОД как услуга”, включающее как инженерные, так и ИТ-системы», – пояснил И. Анисимов. В решение входит не только аппаратная инфраструктура, но и облачная, а также гибкие инструменты софинансирования проекта, в том числе государственно-частное партнерство и опция «ЦОД в рассрочку».

ЦОДы на конвейер

До февраля прошлого года в сегменте малых и средних prefab-ЦОДов на нашем рынке доминировали российские компании, а в сегменте крупных – международные, такие как Vertiv и Schneider Electric, способные предъявить заказчику свои крупные реализованные проекты. Теперь ниша крупных модульных ЦОДов освободилась, и за нее вполне способны побороться российские производители.

С идущими повсеместно процессами цифровизации стране нужно все больше дата-центров. Использование ЦОДов высокой заводской готовности поможет преодолеть текущие трудности и поставить строительство дата-центров на поток. ИКС

PDU RakTek: индивидуальные решения в проектах

Компания RakTek, выход которой на рынок совпал с массовым уходом с него иностранных вендоров, делится своим опытом успешно реализованных проектов.

Выводя на рынок свои PDU, мы решили для получения наиболее релевантных откликов сразу предложить их крупным заказчикам. Как оказалось, это был верный шаг. Чуть более чем за год мы смогли реализовать целый ряд проектов. И этому способствовало то, что всем своим заказчикам PDU мы предоставляем на тестирование, по результатам которого конверсия стремится к 100%!

Заложенные в базовую комплектацию PDU универсальные розетки C13/C19 позволяют заказчикам снять с себя бремя планирования типов и количества выходных розеток. А высокотехнологичные контроллеры, выступающие в качестве интеллектуальной базы блоков распределения питания RakTek, предоставляют широкие возможности мониторинга и управления не только электроснабжением в стойке, но и микроклиматом и доступом в саму стойку – за счет штатных устройств и большой номенклатуры дополнительного периферийного оборудования.

Наши PDU уже можно встретить во многих ЦОДах, как коммерческих, так и корпоративных. Вот лишь несколько реализованных проектов.

В начале 2023 г. мы оснастили своими PDU машинные залы одного из ***операторов сотовой связи***. На фоне относительно стандартных потребностей заказчика нам удалось опередить конкурентов, предоставив надежное решение для распределения питания с функцией мониторинга характеристик электроснабжения на входе в PDU и передачей информации в общую систему DCIM.

Заказчик из госсектора приобрел наши PDU с функционалом мониторинга не только на входе в блок, но и каждого потребителя в отдельности. Дополнительно в поставку вошли наши блоки АВР, предназначенные для размещения в стойке и подключения оборудования с одним источником питания.

Весной этого года мы поставили PDU одному из ***лидеров добывающей отрасли***. Стандартные решения не соответствовали его потребностям, и мы доработали наши блоки, добавив в них помимо идущих в комплекте универсальных розеток C13/C19 с возможностью управления необходимое количество розеток типа Schuko.

Отдельно стоит отметить любовь заказчиков к цветовой маркировке как самих PDU, так и кабелей для подключения нагрузки. Летом для одного из ***крупнейших игроков ИТ-индустрии*** мы отгрузили PDU для строящегося ЦОДа. Для явной идентификации основного и резервного вводов в стойке PDU были окрашены в два разных цвета, и сетевые электрические шнуры имели соответствующие цвета.

По цветовому разнообразию всех превзошел один из ***игроков нефтегазового рынка***, пожелавший окрасить свои PDU в восемь цветов в соответствии с цветом шинопровода, к которому подключен конкретный блок. Такое решение было предусмотрено для сквозной идентификации всей линии электроснабжения. Выбрав PDU компании RakTek, он избежал необходимости дополнительно платить за такую цветовую дифференциацию – при заказе от 10 PDU покраска в требуемый цвет бесплатна. Стоит ли говорить, что объем поставки для данного проекта существенно превосходил это минимальное количество.

Практически все эксперты в области ЦОДов согласны с важностью цветовой маркировки PDU для эксплуатации и обслуживания ЦОДов. Основные преимущества цветных PDU:

- упрощается определение того, к какому источнику питания подключено ИТ-оборудование, устраняются путаница и неудобства при эксплуатации стойки;
- облегчается определение напряжения и потребляемой мощности в источниках питания, что делает распределение нагрузки и управление ею более последовательным и предсказуемым;
- ускоряется поиск и устранение неисправностей (например, отказа ИБП), снижается вероятность человеческой ошибки.

Опыт компании RakTek дает возможность выполнить требования любого заказчика, и не только в плане технических характеристик, но и в вопросах эргономики и удобства эксплуатации. Все это позволяет повысить надежность и отказоустойчивость – ключевые характеристики любого ЦОДа.

Как создать в России инновационную СКС

Александр Брюзгин, директор департамента по работе с ключевыми заказчиками НПП «Гиперлайн», рассказывает о том, как в условиях жесточайших санкций и торговой блокады компании удалось создать по-настоящему прорывную высокотехнологичную СКС для ЦОДов.

– Сегодня заказчики СКС нередко бывают разочарованы новыми решениями. Почему вы считаете, что продукция Hypercore будет принципиально иной?

– Большинство китайских производителей идут по пути копирования успешных западных образцов. Копирование сопровождается сознательным упрощением конструкции для улучшения ценовых показателей и облегчения производственного процесса. Это неизбежно ведет к потере качества, эргономики и эффективности использования. В результате вы относительно недорого получаете продукт, который номинально выполняет свою функцию, но делает это плохо, особенно по сравнению с продукцией ушедших лидеров отрасли.

НПП «Гиперлайн» избрало другой путь. Как вы знаете, мы не так давно заявили о новом бренде – Hypercore. Сначала мы провели расширенное обсуждение продукта с потенциальными партнерами и заказчиками, собрали и систематизировали их мнения. Затем внимательно проанализировали тенденции в развитии СКС для ЦОДов и сравнили их с трендами рынка активного оборудования. Мы не можем разрабатывать продукт, опираясь только на пожелания потребителей, поскольку они в основном судят по тем продуктам, которые используют сейчас, и не всегда представляют, что им понадобится завтра. Нащупать это «завтра», превратить его в продукт, который ответит на только зарождающиеся потребности, – вот задача настоящего производителя, задача творца.

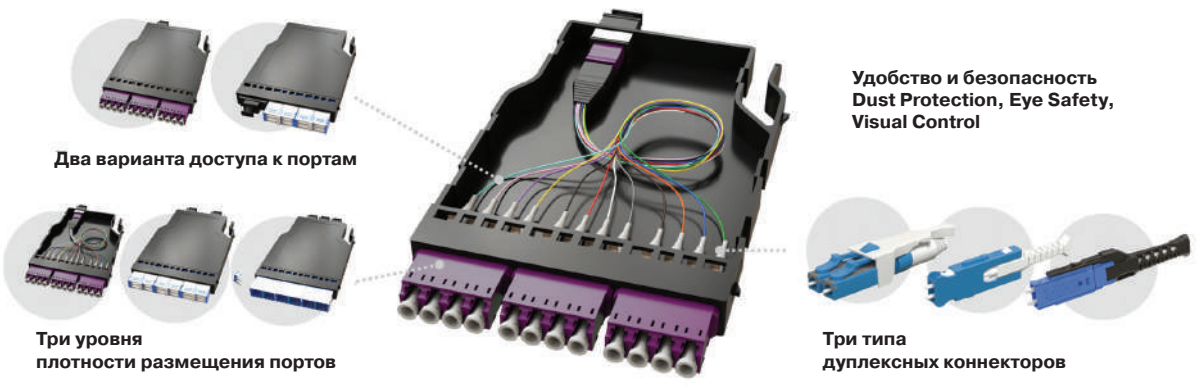
При разработке нашего продукта – оптической полки Hypercore и ее наполнения – мы с самого начала исходили из того, что будем создавать премиальный продукт. То есть продукт, обладающий самыми передовыми техническими характеристиками, лучшей эргономикой и удобством монтажа и обслуживания. Кроме того, продукт изначально задумывался как часть решения end-to-end для современных ЦОДов, в том числе для топологии Spine – Leaf.

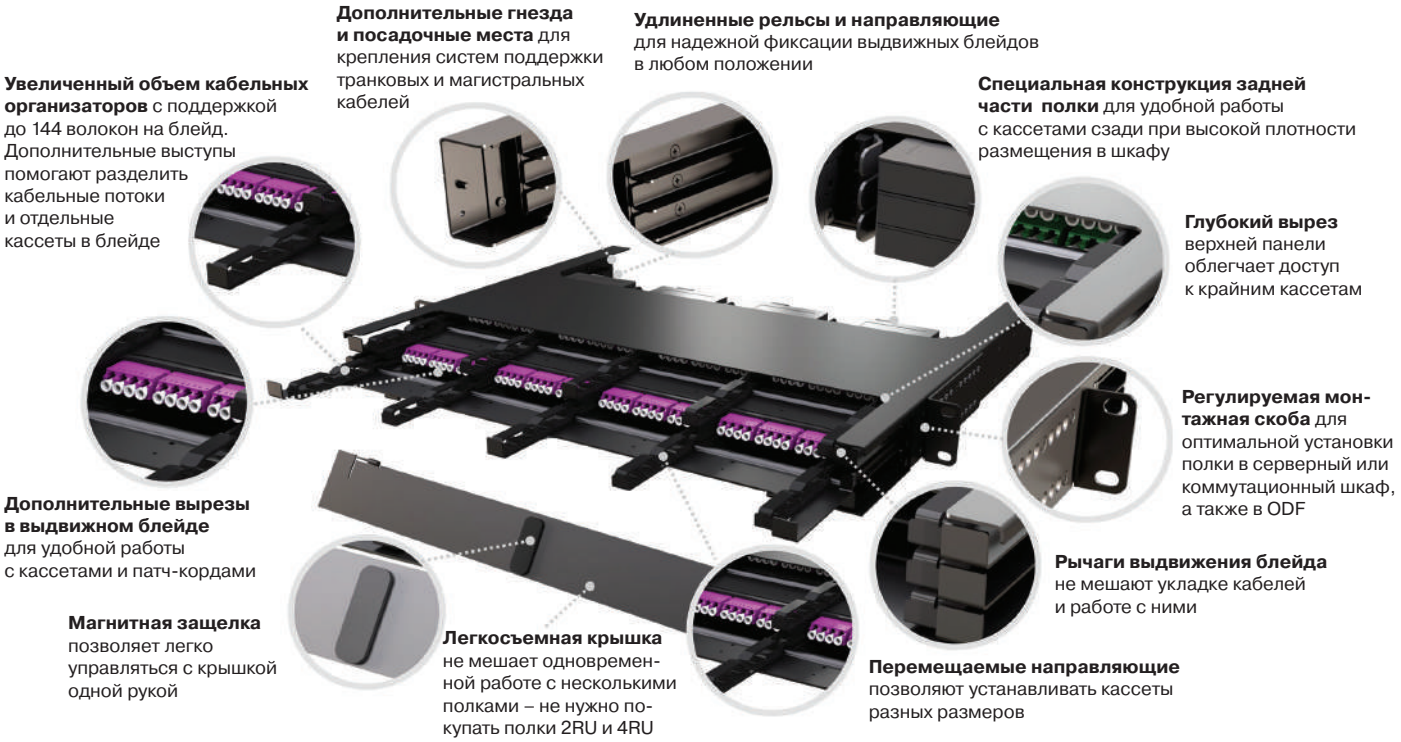
Наконец, мы разработали концепцию *суперуниверсальности*. Она легла в основу философии Hypercore. Наш продукт (оптическая полка с кассетами в системе выдвижных блейдов) может успешно применяться практически в любом месте ЦОДа – от главного оптического кросса до одиночной полки в серверном шкафу ToR. Мы можем разместить в нашем продукте любые системы оптических соединений – от традиционных LC и MPO до систем нового поколения (VSFF). Таким образом, он сможет оставаться актуальным много лет и даст возможность нашим заказчикам провести модернизацию и смену поколений активного оборудования и СКС без замены наших конструктивов.

Серьезное преимущество универсальности состоит в том, что вы получаете унифицированную спецификацию и структуру СКС, вам требуется меньше ЗИП и т.п. Иными словами, универсальность = повышенная надежность + гибкость использования. Вместе с тем универсальность – это возможность сконфигурировать продукт для конкретного ЦОДа с любой спецификой.

– Какие же основные пожелания заказчиков, специалистов, занимающихся эксплуатацией СКС, удалось учесть?

– Назову лишь некоторые. Это удобство работы с полками и кассетами сзади при размещении большого количества кассет вместе (в оптическом кроссе); удобство работы с высокоплотными решениями (144 волокна в 1RU и выше) с передней панели; возможность использования полок в специализированном шкафу ODF глубиной не более 300 мм; возможность изменения конфигурации кассет





(использования кассет различного форм-фактора); открывание крышки одной рукой и т.д.

Мы изначально заложили в продукт и его компоненты самые жесткие требования: он должен обеспечивать максимальный запас по бюджету потерь с тем, чтобы безусловно соответствовать требованиям заказчика при любых условиях монтажа и эксплуатации. Этот запас может показаться излишним, так как любое активное оборудование рассчитано на определенный бюджет потерь в канале и не станет работать быстрее, если мы этот бюджет снизим, скажем, вдвое. Мы рассматриваем низкий показатель вносимых потерь (IL) как запас прочности, который наряду с более совершенными с точки зрения используемых материалов и технологий компонентами гарантирует нашим потребителям стабильность параметров в течение продолжительного срока службы.

Отмечу также, что все адаптеры в наших кассетах, будь то LC, MPO или SN, обладают встроенными внутренними шторками. Эти шторки открываются только соответствующим коннектором в процессе соединения. Кроме своей основной функции – защиты от пыли – шторки выполняют функцию защиты глаз от лазерного излучения.

Одним из основных факторов выбора в пользу компонентов Senko явились совершенные ферулы для всей линейки оптических коннекторов. Эти ферулы в наибольшей степени определяют возможности снижения показателя IL при производстве оптических продуктов. Хочу подчеркнуть, что новое поколение коннекторов Senko открывает нам путь к решениям для ЦОДов производительностью 400, 800 Гбит/с и 1,6 Тбит/с.

– Где сейчас размещается производство?

– На данный момент у нас мелкосерийное производство, которое имеет свои ограничения. Мы уже выпускаем продукт и готовы предоставить образцы для опробования и тестирования нашими партнерами и клиентами для того, чтобы они могли принять решение о его использовании в ближайших проектах. Мы также рассчитываем получить отзывы для дальнейшего развития продукта.

При переходе к серийному производству мы будем задействовать собственные производственные площадки в Москве и Калужской области и, конечно, контрактное производство. Мы уже задумываемся о соответствующих площадках как в России, так и за рубежом.

– Как собираетесь контролировать и гарантировать качество своего решения?

– Вы задали важный и одновременно сложный вопрос. Контроль качества – это показатель зрелости культуры производства в целом.

Критические компоненты нашего продукта изготавливаются на производствах с уже налаженной системой контроля качества. Что касается гарантии на нашу продукцию, то НПП «Гиперлайн» как ответственный производитель следует всем мировым правилам и нормам. При этом, являясь российским производителем и имея локальное производство и склад, мы готовы обеспечить кратчайшие сроки замены вышедших из строя компонентов. Также мы разрабатываем дополнительные сервисные программы с учетом потребностей клиентов ЦОДов.

– Традиционный вопрос о планах. Что в вашей «дорожной карте»?

– В I квартале 2024 г. мы представим рынку революционное решение от Hypercore – оптическую СКС для ЦОДов нового поколения. Мы снизим бюджет потерь в каналах оптической СКС наполовину и сделаем это без увеличения цены системы.

Подробнее как об имеющихся, так и о будущих решениях вы можете узнать у наших представителей 12 сентября на конференции «ЦОД» в Москве.

Ближайшие и среднесрочные перспективы развития СКС для ЦОДов

Андрей Семенов, профессор, МТУСИ

Для того чтобы СКС, развернутая в ЦОДе, могла эффективно обслуживать его вычислительные мощности и сегодня, и через 10 лет, она должна быть построена в соответствии с трендами развития отрасли.

Машинный зал ЦОДа представляет собой сложную техническую систему. Та ее часть, которая отвечает за хранение и обработку данных, для достижения максимальной технико-экономической эффективности в целом строится с привлечением проверенной временем модели взаимодействия открытых систем OSI. Ее физический уровень в соответствии с положениями стандартов ISO/IEC 11801-5:2017, ANSI/TIA-942C и ГОСТ Р 59486-2021 реализуется в виде структурированной кабельной системы (СКС).

При создании СКС необходимо не только удовлетворять сегодняшние потребности, но и не допустить ее морального, структурного и тем более физического устаревания на протяжении всего ожидаемого срока эксплуатации, т.е. по меньшей мере 10 лет.

Физическое устаревание не проявляется при построении СКС на высококачественной элементной базе с запасами по пропускной способности. Структурное устаревание предотвращается проектными приемами: введением необходимой функциональной избыточности, применением легко адаптируемых к новым потребностям конфигураций кабельных трактов и т.п.

Отсутствие морального устаревания обеспечить существенно сложнее. Из-за большого количества факторов и жестких начальных условий риск выбора неудачного технического решения при построении информационной проводки машинного зала высок. Единственный способ его снизить – учитывать основные тренды развития отрасли. Рассмотрим магистральные направления совершенствования этого сегмента слаботочной кабельной техники.

Предельная протяженность стационарной линии

С точки зрения развертывания кабельной системы характерная топологическая особенность ЦОДа, существенно отличающая его от офисных пространств, – геометрическая компактность. Она обусловлена применением воздушного охлаждения для утилизации больших объемов теплоты, вырабатываемой серверами и активным сетевым оборудованием. Высокое потребление энергии сетевой техникой неизбежно из-за ее функционирования в режиме разгона для достижения максимального быстродействия. При этом по мере увеличения площади машинного зала КПД системы воздушного охлаждения падает.

Площадь машинного зала ЦОДа жестко связана с количеством устанавливаемых в нем стоек. В качестве типового можно рассматривать машзал прямоугольной формы с соотношением сторон 1:3, вмещающий 320 стоек. Оценкой сверху максимальной протяженности стационарной линии машзала может служить его полупериметр. Исходя из того, что каждая стойка занимает примерно 2,6 кв. м, и добавляя 15% на центральный кросс и т.п., пу-

тем несложных расчетов получим, что максимальная протяженность стационарной линии не превысит 72 м. Таким образом, 300-метровая нормативная протяженность оптических магистралей офисных СКС для рассматриваемой области применения избыточна, и ее допустимо уменьшить до 70–150 м.

Противоречие между нормативными положениями стандарта-прототипа, которые из соображений гармонизации без изменений используются для цодовских СКС, и фактическими потребностями практики устраняется переходом на нормирование предельно допустимой длины тракта «по приложению». За счет уменьшения предельной протяженности тракта появляется возможность задействовать для организации информационной проводки машинного зала экономически заметно более выгодную многомодовую элементную базу.

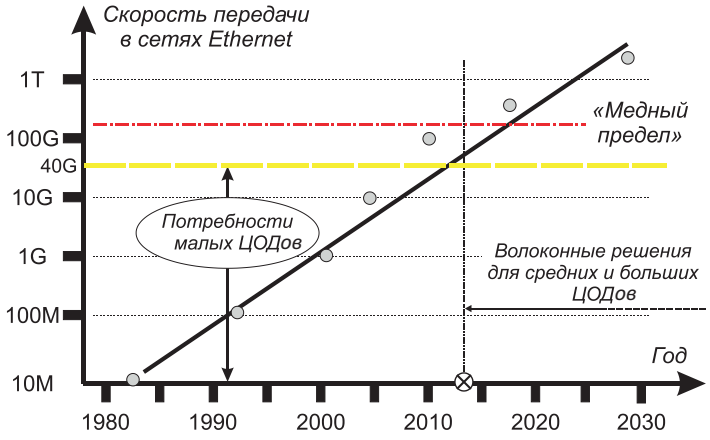
Схема Base8 как основа для формирования параллельной передачи

Линии связи машинного зала строятся по схеме параллельной передачи, поскольку из-за ограниченного быстродействия современной электроники (тактовая частота не превышает 30–50 ГГц) это единственный способ нарастить скорость информационного обмена. Вместе с тем в ЦОДе нет необходимости непосредственно взаимодействовать с пользователем-человеком в качестве источника и потребителя данных и соответственно нет нужды ориентироваться на его возможности восприятия информации.

В рамках параллельной передачи сообщение разбивается на несколько составляющих, каждая из которых передается по отдельному субканалу, и затем восстанавливается на приемном конце. При формировании линейного сигнала используется чистая амплитудно-импульсная или комбинированная амплитудно-фазовая импульсная модуляции. Они позволяют передавать одновременно до четырех бит данных за один тактовый интервал. Для увеличения количества субканалов можно обратиться к технологии SWDM. В этом случае при организации линейной части канала связи по схеме Base8 получаем следующую оценку верхней границы достижимой скорости передачи:

$$W = 25\ ГГц \times 4\ волокна \times 4\ бит/такт \times 4\ длины\ волны\ SWDM = 1{,}6\ Тбит$$

Обеспечиваемый схемой Base8 скоростной запас таков, что риск морального устаревания построенной с ее использованием СКС в горизонте 10 лет практически нулевой. Отрасль еще не приступила к освоению скоростей даже 800 Гбит/с, а реальная потребность в скоростях передачи свыше 1,8 Тбит/с возникнет не ранее 2030–2035 гг. (рис. 1).



▲ **Рис. 1. Темпы роста скоростей передачи данных в ЦОДах**

Перспективы волокна категории OM5

Вследствие геометрической компактности машзалов ЦОДов протяженность стационарных линий СКС невелика (около 30 м), и их можно строить на экономичной многомодовой технике. Для создания физического уровня канала связи целесообразно использовать многомодовые оптические кабели категории OM5. Соответствующее волокно можно рассматривать как дальнейшее развитие техники категории OM4. Световоды OM5 обратно совместимы с волокнами OM4 и отличаются от них только нормированием коэффициента широкополосности на длине волны 953 нм. Переход на OM5 выгоден тем, что позволяет увеличить техническую эффективность как минимум на треть*.

Сильные стороны многомодового волокна категории OM5 проявляются на скоростях 800 Гбит/с и выше, т.е. в тех случаях, когда используется полноценное спектральное мультиплексирование по технологии SWDM. Сегодня такие решения востребованы скорее фрагментарно. Тем не менее с учетом перспектив развития техники и ожидаемого срока эксплуатации ЦОДа волокно OM5 целесообразно закладывать в проекты уже сейчас, особенно для объектов с увеличенной протяженностью линий. Таковыми являются ЦОДы с количеством стоек 150 и более либо построенные на схеме Spine – Leaf.

Новые типы оптических разъемов

Тракты оптической параллельной передачи, согласно стандартам, реализуются на соединителях MPO/MTP. Разъем имеет переделочную конструкцию и ряд принципиальных недостатков, от которых свободны новые изделия груп-

*Семенов А.Б., Былина М.С. Техническая эффективность параллельных многомодовых оптических кабельных трактов категории OM5 // Информационно-технологический вестник. 2017. № 4 (14). С. 91–101.

пы VSFF с вертикальным дизайном. Последние ориентированы на схему Base8 и легко решают проблему полярности формируемых трактов, упрощают агрегацию каналов и построение отказоустойчивых структур, а также способствуют снижению потерь в тракте за счет уменьшения количества точек сращивания.

Соблюдение полярности обеспечивается благодаря дуплексной структуре отдельной вилки VSFF-разъема, которые могут комбинироваться в произвольном порядке и с любой ориентацией. При необходимости несколько (до четырех) вилок собираются в групповую путем установки в общую пластиковую фиксирующую оправку.

Простота доступа к отдельной вилке решает также задачу агрегации отдельных каналов группового сигнала Ethernet при построении отказоустойчивых структур.

Наиболее известные элементы этой группы, доведенные до уровня серийного предложения, – это коннекторы MDC (Mini Duplex Connector) американской компании US Conec и SN (Senko Nano) японской компании Senko. Отрасль рассматривает это направление как весьма перспективное, о чем косвенно свидетельствует появление аналогичной разработки DPO китайской компании Unikit. Сильная сторона DPO – оригинальное решение проблемы совместимости с MDC и SN: для подключения их вилок достаточно установить вкладыш-переходник в розеточное гнездо.

Еще одно преимущество соединителей группы VSFF – существенное упрощение плавной миграции на более высокие скорости передачи. Для этого служит типовой механизм агрегации отдельных каналов группового сигнала Ethernet, который позволяет заменять аппаратуру только на одном из концов линии.

Необходимость перехода на схему Spine – Leaf

Обеспечение требуемой скорости и глубины обработки пользовательских запросов, т.е. в конечном счете качества функционирования ЦОДа, зачастую требует организации параллельных вычислений. Для этого несколько физически различных серверов нужно объединить в единую структуру коммутаторами.

Любой коммутатор вносит задержку в передаваемый сигнал. Ее конечная величина определяется:

- принятием решения о передаче сигналов «0» и «1» в середине тактового интервала для снижения вероятности ошибки (задержка на половину такта);
- неопределенностью поступления входного сигнала на порт коммутатора и необходимостью ее исключения привязкой входящего импульса к соответствующему стробу внутреннего тактового генератора;
- конечным временем записи и считывания поступающего/передаваемого сигнала в/из внутренней памяти коммутатора;
- задержкой чтения адресной информации из поступающего кадра Ethernet для определения порта назначения, проявляющейся вне зависимости от используемого метода коммутации (рис. 2).

Суммарное время чисто аппаратурной задержки сопоставимо с задержкой физического распространения сигнала в типовых кабельных трактах машинного зала ЦОДа. Механизм формирования этой задержки в принципе не позволяет сделать ее меньше некоторого довольно большого значения. Поэтому единственный способ повысить быстродействие распределенной вычислительной структуры в целом – уменьшить количество коммутаторов в цепи передачи сигнала от одного сервера к другому. Этого можно добиться отказом от классической трехуровневой модели информационной инфраструктуры в пользу двухуровневой. Реализующие ее структуры выделяются в отдельную группу Spine – Leaf.

Переход к архитектуре Spine – Leaf сопровождается существенными изменениями как самой СКС, так и применяемого в ней коммутационного оборудования. Это обусловлено:

- увеличенным количеством линий из-за необходимости обеспечения связи «каждый с каждым»;
- необходимостью резервирования отдельных линий для повышения общей эксплуатационной надежности ЦОДа;
- сложностями добавления новых линий при расширении ЦОДа и введении новых серверов и/или коммутаторов в существующую структуру.

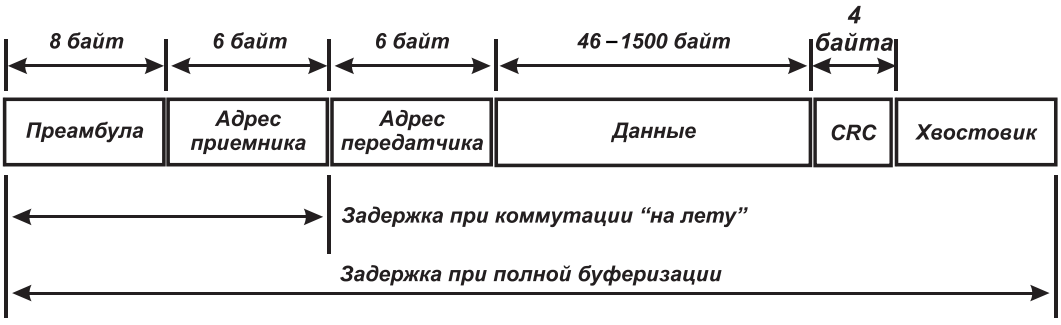


Рис. 2. ►
Схема возникновения задержки при обработке кадра Ethernet в коммутаторе

Наиболее простой и экономичный способ решения этих проблем – целенаправленное введение в состав СКС дополнительного центрального кросса*.

Распространение архитектуры Spine – Leaf оказывает мощное стимулирующее воздействие на разработку специализированных центральных кроссов. Причем это воздействие намного сильнее, чем то давление, которое оказывает на рынок естественный рост средних и крупных по количеству стоек ЦОДов.

Важно, что повышенный расход кабеля из-за роста количества линий и увеличения их средней длины не сопровождается критическим давлением на бюджет проекта. Сказывается то, что доля СКС в общем объеме капитальных затрат при существующей схеме организации проводки не превышает 5% и вполне может быть увеличена для придания ЦОДу новых технических свойств.

Перспективы электропроводной техники

Сегодня наиболее широкополосные электропроводные линии относятся к классу G и реализуются на элементной базе категории 8. Они обеспечивают скорость передачи 40 Гбит/с и изначально ориентированы на применение в ЦОДах. Их основные особенности:

- возможность построения только простых двухконнекторных структур со схемой коммутации интерконнекта;
- уменьшение максимальной протяженности тракта до 28–32 м в зависимости от калибра гибких проводников шнуров;
- применение только экранированной техники для эффективного подавления межкабельной переходной помехи.

*Подробнее см. Семенов А. Архитектура Spine – Leaf в ЦОДах: зачем нужна и как реализовать // «ИКС» № 4'2022, с. 44.

При необходимости как скорость передачи, так и предельная протяженность симметричного тракта могут быть увеличены до 100 Гбит/с и 100 м соответственно. При этом дальнейшее существенное наращивание скорости даже при сокращении предельной протяженности тракта становится проблематичным. Это обстоятельство получило название медного предела (см. рис. 1). Поскольку он был достигнут уже в начале второго десятилетия текущего века, перспективы применения электропроводной техники в крупных ЦОДах отсутствуют. Тем не менее при появлении соответствующего активного сетевого оборудования она будет востребована в малых ЦОДах.

■■■

ЦОДы – основной драйвер наращивания скорости передачи данных по кабельным трактам СКС, в первую очередь по волоконно-оптическим. В перспективе ожидается выход в терабитные скорости передачи.

При построении кабельных трактов волоконно-оптической подсистемы в качестве основной целесообразно применять схему Base8, которая обеспечивает отсутствие морального устаревания по крайней мере в ближайшей и среднесрочной перспективе.

Существующее многомодовое волокно категории OM5 по своим параметрам вполне удовлетворяет текущим и перспективным потребностям; острой необходимости в разработке новых типов волокна нет.

Переход к скоростям 400 Гбит/с и выше целесообразно совместить с широким внедрением разъемов нового типа из группы VSFF; наличие конкурирующих разработок должно положительно сказаться на скорости внедрения этой техники в широкую инженерную практику.

Выполнение СКС на базе кабелей из витых пар имеет смысл только в небольших ЦОДах. ИКС

EMILINK: бренды NTSS и KOSCAB становятся самостоятельными

Группа компаний EMILINK на пороге серьезных перемен. Она уходит от прямых продаж и мультибрендового продвижения своей продукции. Теперь принадлежащие ей бренды NTSS и KOSCAB будут развиваться собственными путями.

Не так давно российский производитель телекоммуникационного оборудования сообщал о переезде главного офиса в центр столицы. Теперь вслед за внешними переменами настал черед внутренней трансформации. О предстоящих переменах рассказывает основатель группы компаний EMILINK **Андрей Зуев**.

– ГК EMILINK принадлежат бренды NTSS, под которым мы выпускаем пассивное телекоммуникационное и серверное оборудование, и KOSCAB – производство оптического кабеля. Основные продажи оборудования и маркетинговое продвижение раньше шли через сайт emilink.ru. Теперь мы решили, что NTSS и KOSCAB будут развиваться как самостоятельные бренды. У каждого из них будет своя бизнес-политика, независимая от EMILINK, свои партнеры, свой дистрибьюторский канал. Можно сказать, что это трансформация в духе новых веяний.

– А как будет развиваться EMILINK?

– EMILINK дистанцируется от прямых продаж. Все, что касается бизнеса в России, будет происходить через партнеров. Emilink.ru превратится в сайт-визитку. Основными порталами станут ntss.ru и koscab.ru. Это позволит нам четко разделить бизнес с партнерами, стать максимально прозрачными. Также мы будем выделять отдельный бюджет для маркетингового продвижения этих направлений совместно с партнерами, с дистрибьюторами. Кроме того, в EMILINK мы сворачиваем тендерную работу. Тендерный отдел в ближайшие несколько месяцев перепрофилируется в отдел сопровождения ключевых партнеров, т.е. наших дистрибьюторов.

– Смелый, но своевременный и несомненно важный для компании шаг.

– Да, мы поняли, что NTSS и KOSCAB стали уже настолько самостоятельными, что необходимо переходить на новый уровень!

Андрей Зуев отметил, что сегодня в каждом направлении сформированы сильные команды специалистов, растут производственные мощности, расширяются ассортимент и география присутствия компании, как в России, так и в СНГ. О том, какие шаги по развитию бизнеса предпринимают производители продукции, выпускаемой под брендами NTSS и KOSCAB, мы попросили рассказать команду.

***Евгений Плесовских**, генеральный директор ГК EMILINK:* В прошлом году мы внедрили систему ERP. В ближайших планах – запуск B2B-площадки, на которой корпоративные клиенты смогут видеть новости компании, новинки, акции, персональные условия, статус оформления заявок, складские остатки. Что касается производства, то в этом году мы открыли в Костроме еще одну площадку, где собираем медные и оптические патч-корды. Для площадки металлообработки в Костроме же закупаем дополнительные гибочные и координатно-пробивные станки и другое оборудование. По собственным проектам модернизируем полуавтоматическую линию полимерной окраски. В дальнейшем планируем роботизировать наши площадки. Мы входим в реестр «Ростелекома» как поставщик кабельной продукции, некоторые виды кабеля прошли испытания в лаборатории МГТС, также наша продукция внесена в реестр Минпромторга. Активно работаем как с коммерческими структурами, так и с государственными. Считаю, что мы – один из ключевых игроков на рынке.

***Максим Ковалев**, продакт-менеджер NTSS по направлению металлообработки*: Шкафы и стойки под брендом NTSS производятся уже более восьми лет, но только последние четыре года стали прорывными. Если пять лет назад мы выпускали 100–150 единиц ежемесячно, то за последние два года – более 2000 шт. В среднем конструкция шкафа «живет» на рынке ЦОДов около трех лет. Поэтому мы постоянно обновляем модели – выпускаем новые или улучшаем существующие с учетом современных технологий. При этом мы отказались от копирования чужих разработок. На основе своего опыта, идей, отзывов клиентов прорабатываем различные опытные образцы и выводим на рынок собственные решения. Мало кто из российских компаний может похвастаться таким подходом. Что касается систем изоляции NTSS, то еще четыре года назад они практически не производились, а сейчас уже сменились два поколения. Например, конструкций типа «факел» за последний год мы выпустили на 100% больше, чем четыре года назад, и на 60% больше, чем двумя годами ранее.

***Елена Лобанова**, директор по развитию бренда NTSS*: Считаю большим достижением, что за прошедший год мы навели порядок в направлении СКС. Мы глобально изменили структуру работы по проектам, оптимизировали защиту проектов, расширили ассортиментную матрицу, увеличили складские запасы. И главное – провели огромную работу по улучшению качества продукции. Если ранее мы конкурировали с бюджетными брендами и выпускали более дешевый продукт, то теперь ориентируемся на качество дорогих брендов, ушедших с российского рынка. Ввели, например, дополнительный контроль качества на производственных площадках – 100%-ное тестирование по нескольким параметрам патч-кордов серии «Премиум». В итоге – положительные отзывы покупателей и рост продаж. Так, в первом полугодии продажи NTSS «Стандарт» увеличились на 70%, а «Премиум» – на 50%. В планах по развитию СКС – расширение ассортимента медных компонентов серий «Стандарт» и «Премиум», разработка новых систем высокой плотности.

***Сергей Волков**, продакт-менеджер NTSS по кабеленесущим системам*: Производство систем прокладки кабеля запустили только в начале текущего года. Начали с четырех направлений: пластиковые кабельные каналы, проволочные лотки, перфорированные лотки и кабельные каналы для оптических сетей (так называемые желтые кабельные каналы). Первые итоги: особенно успешными оказались перфорированные кабельные каналы. Буквально сейчас отгружается очередная машина для трех контейнерных ЦОДов. Большую партию желтых лотков подготовили для отправки в дата-центр в Крым. Заказов с каждым днем все больше. Качество, которое мы предлагаем, в соотношении с нашей ценой очень привлекательно для заказчиков. К тому же у нас российское производство. В ближайшей перспективе в ассортимент планируем добавить еще несколько видов металлических лотков – неперфорированные и лестничные. Соотношение цены и качества сохраним.

***Борис Васильковский**, продакт-менеджер NTSS по PDU*: Направление блоков распределения питания (PDU) считаю сегодня одним из самых перспективных. В 2022 г. мы провели большую работу, плоды которой увидели уже в первом полугодии, и по итогам года ожидаем, что продажи вырастут многократно. Например, мы выиграли ряд конкурсов на поставку PDU в крупные ЦОДы. Производим вертикальные PDU в 19-дюймовом исполнении, базовые и интеллектуальные. Постоянно модернизируем и улучшаем наши устройства. Ведем работу над интеллектуальными PDU полностью российского производства, с отечественными деталями и программным обеспечением собственной разработки. На складе всегда имеем запас бестселлеров, а по заказным позициям срок поставки не превышает шести недель для интеллектуальных и трех – для базовых версий PDU. Появились первые дистрибьюторы в ближнем зарубежье.

***Мария Мишанина**, руководитель проектного отдела NTSS*: С прошлого года мы предоставляем услуги построения ЦОДа под ключ: не только изготовим и доставим все необходимое оборудование, но и установим. В этом году мы успешно реализовали ряд проектов по модульным ЦОДам для компании GreenMDC. А в планах совершенно новый для нас проект – поставка заказчику серверных шкафов, уже «расшитых» СКС. Отмечу, что наш проектный отдел теперь самостоятельно составляет рабочую документацию – появились необходимые ресурсы. Мы начинаем тесно сотрудничать с проектными организациями. Я знаю, что с нами хотят работать. Те, с кем мы уже реализовывали проекты, оставляют нам отличные отзывы. Нам звонят по рекомендациям и говорят: «Вас посоветовали, хотим работать именно с вами». Это очень приятно!

***Артем Соловьев**, директор по развитию бренда KOSCAB*: Бренд KOSCAB (завод «Костромакабель») развивается отличными темпами. За год производство оптического кабеля, согласно плану, выросло на 40%. По выпуску сопутствующих товаров мы уже вышли на уровень 2022 г. И возможности далеко не исчерпаны. Производство имеет огромный потенциал и пока загружено только на 50%. Мы активно работаем с дилерами, расширяем присутствие в Сибири, СНГ, нацелены на Северо-Кавказский и Северо-Западный федеральные округа. Открыты к сотрудничеству с новыми партнерами. Имеем большие запасы на складах, постоянно модернизируем производство. Так, планируем закупку еще одной линии для выпуска локальных типов кабеля, кабелей для канализации, дроп-кабелей. Строго следим, чтобы увеличение мощностей не шло в ущерб качеству. Высокий уровень качества – то, почему нас выбирают. За пять лет работы помню лишь две претензии из-за брака, в обоих случаях брак оперативно устранили. Мобильность, гибкость, индивидуальный подход к партнеру, ценовая политика – считаю, что в этом мы тоже лучшие!

СКС, достойная войти в топ

Российская компания Eurolan анонсировала выпуск оптической СКС высокой плотности с использованием компонентов лучшего европейского качества. Подробностями делится руководитель направления Eurolan CORE Валерий Никитин.

– Валерий, расскажите о вашей компании.

– Eurolan – ведущая российская компания, работающая на ИТ-рынке более 20 лет и поставляющая продукцию для построения структурированных кабельных систем зданий и дата-центров. Компания самостоятельно разрабатывает решения и производит их на различных площадках. Для разработки и внедрения новых продуктов у компании есть R&D-центр в Москве. Он занимается созданием продуктов, которые удовлетворяют спрос на оборудование, востребованное на рынке.

Производственные площадки располагаются в России, Китае и Израиле, на Тайване и в Беларуси, что выгодно с точки зрения доступности компонентной базы.

– Как изменилась политика компании после ухода с российского рынка зарубежных вендоров?

– Политика Eurolan формировалась на протяжении более чем 20 лет и сохранила свои ключевые ориентиры: надежность, стабильность и высокое качество. С уходом зарубежных вендоров обращений и запросов от партнеров и клиентов стало значительно больше, что, конечно же, увеличило нагрузку на наших специалистов. Но наличие собственного R&D-центра и широкой партнерской сети позволило нам без потери качества выполнять крупные проекты и отвечать на возросшее число запросов.

– Какие новые запросы сформировал российский рынок в 2023 г.?

– Ключевым направлением для компании Eurolan были и остаются поддержка и развитие сети проектных партнеров. События 2022 г. подтвердили верность выбранной стратегии.

Eurolan заметила растущий тренд замены решений западных производителей на более доступные и локально ориентированные альтернативы и предложила продукты с учетом новых запросов российского рынка, в частности, новое высокоплотное решение CORE для дата-центров, которое соответствует требованиям самых взыскательных заказчиков.

– С какими трудностями столкнулась компания при разработке нового решения?

– Для того чтобы приступить к разработке такого объемного решения, как оптическая СКС для ЦОДов, мы расширили свой R&D-центр и дополнили команду Eurolan экспертами рынка, имеющими опыт сотрудничества с мировыми лидерами – поставщиками «тяжелых» систем для оптических сетей.

Этими экспертами стали специалисты из компании Lindex, которая не только является эксклюзивным дистрибьютором Eurolan, но и долгое время сотрудничала с мировыми производителями СКС для ЦОДов в плане дистрибуции и проектных поставок высокоплотных оптических СКС. Из Lindex в команду Eurolan перешли эксперты с богатым, более чем десятилетним опытом реализации крупных проектов пассивной инфраструктуры ЦОДов и опытом в области эксплуатации подобных систем.

На планирование, разработку и реализацию ушло больше года, поскольку Eurolan изначально предъявляла высокие требования к качеству продукции и к возможностям производственных площадок выполнить все технические требования.

Конечно, мы обращались в Китай, но местные производители, использующие в работе стандартные компоненты, не смогли реализовать наше техническое задание.

Продолжив поиски, мы нашли проектную группу в Израиле, способную создать решение в соответствии с нашими требованиями. Получили пилотные образцы, внесли корректировки, и вот появился продукт Eurolan CORE, который на данный момент собирается на площадке в Израиле. Мы полностью готовы к поставкам этого решения и реализации на его основе проектов заказчиков в области построения СКС для ЦОДов.

– В чем особенности нового решения – оптической СКС Eurolan CORE?

– Модульная претерминированная оптоволоконная система сверхвысокой плотности Eurolan CORE предназначена для работы в дата-центрах. Решение обеспечивает высокую плотность соединений благодаря модульной структуре, которая облегчает процесс перемещения, добавления и изменения оборудования. Eurolan CORE предоставляет простой доступ к портам, имеет встроенную систему организации кабелей, а также отличается меньшими требованиями к пространству для монтажа по сравнению с другими оптоволоконными кабельными системами.

Оптические системы Eurolan CORE рассчитаны на использование 12-волоконных оптических линий CORE 12 и 8-волоконных линий CORE 8. 12-волоконные линии – наиболее популярные сегодня системы для приложений с высокими скоростями передачи данных. 8-волоконные линии обеспечивают максимальную эффективность использования волокон и оптимальны для перехода на более высокие скорости передачи данных вплоть до 1600 Гбит/с.

Основной элемент системы Eurolan CORE – центральный кросс для главной зоны распределения (Main Distribution Area, MDA). Именно его создание заняло бóльшую часть времени, затраченного R&D-центром на разработку всего решения. Это решение должно было обеспечить размещение большого количества оптических портов с возможностью эффективно управлять каждым из них. Центральный кросс играет важную роль в качественном проектировании системы СКС ЦОДа. Он позволяет сконцентрировать все порты оптического оборудования в одном месте и управлять каждым портом по отдельности.

Порты подключения активного оборудования расположены в одной половине шкафа главной зоны распределения, порты подключения серверов – в другой. В пределах этой стойки кросс-коммутации проводится соединение нужных портов. В центральном кроссе есть необходимые зоновые панели разных номинаций и претерминированные решения в виде кассет и патч-кордов.

Уникальность системы – использование во всех зонах унифицированных компонентов: кассет одного типа, патч-кордов одного типа и одинаковой длины. Заказчику не нужно иметь ЗИП с большой номенклатурой. Для обслуживания центральной зоны требуется кабель длиной 4 м, который в зависимости от выбранной архитектуры содержит 8 или 12 волокон.

Другая важная особенность – использование компонентной базы только от известных производителей. Компоненты поставляются компаниями – мировыми лидерами рынка СКС.

Стоит отметить универсальность решения, которое позволяет без внесения серьезных изменений в сеть обеспечивать скорость от 1 до 1600 Гбит/с. Магистрали, в которых используются наши кассеты, строятся один раз, а потом по мере развития технологий переключаются на более высокоскоростные режимы. Eurolan CORE поддерживает все технологии, представленные на рынке.

Высокая плотность достигается минимизацией форм-фактора кассеты и грамотным исполнением панели. Центральный кросс способен вместить более 5 тыс. оптических волокон с разъемом LC, а с разъемом MTP – 65 тыс. волокон. Помимо прочего решение обеспечивает управление коммутацией. Конструкция позволяет легко переключать до 3 тыс. соединяющих разъемы шнуров. Панели выдвигаются, открывая удобный доступ к патч-корду. Для перекоммутации не нужны инструменты или специальные патч-корды. Эксплуатация не вызывает проблем даже у персонала, не имеющего большого опыта работы.

– Как организована сервисная поддержка вашей продукции по стране? Как контролируете квалификацию специалистов?

– Компания Eurolan предлагает двухуровневую сервисную модель, широко распространенную в ИТ-отрасли. Первый уровень поддержки обеспечивает эксклюзивный дистрибьютор Lindex, второй уровень ложится на сервисное подразделение Eurolan. Важный элемент успешности этой модели – высокий уровень компетенций сотрудников дистрибьютора, которые проходят ежегодное обязательное обучение и тестирование в компании Eurolan.

Для партнеров авторизованных инсталляторов организованы онлайн-обучение и тестирование, а также ежегодные слеты партнеров Eurolan на конференции Eurolan Day с обзорами стандартов и тенденций отрасли, презентациями обновленных продуктов и решений компании. Мероприятия проходят в ключевых регионах России, Казахстана и Белоруссии.

– На каких потребителей рассчитаны решения компании?

– Eurolan давно предлагает медные и оптические решения для офисных СКС. Однако в свете резких изменений на рынке компания провела трансформацию, чтобы соответствовать новым запросам клиентов, особенно тех, кто имеет обширные системы хранения данных, требующие использования оптики и сложной коммутационной инфраструктуры.

Анонсированное в мае нынешнего года флагманское решение Eurolan CORE – ядро оптической кабельной системы. Оптика стала серьезным конкурентом «меди» и находит все более широкое применение на российских предприятиях, в банках и дата-центрах, прежде всего предоставляющих услуги по модели colocation.

– Каковы финансовые результаты прошлого года и ваши основные направления деятельности?

– В прошлом году мы достигли значительного роста продаж: согласно отчетам Lindex, он составил 76%. После ухода крупных игроков с рынка СКС Eurolan смогла проявить себя как зрелая компания, которая оперативно и без потери качества нарастила объемы поставок предлагаемых продуктов и решений. Решения Eurolan пользуются спросом у широкого круга заказчиков.

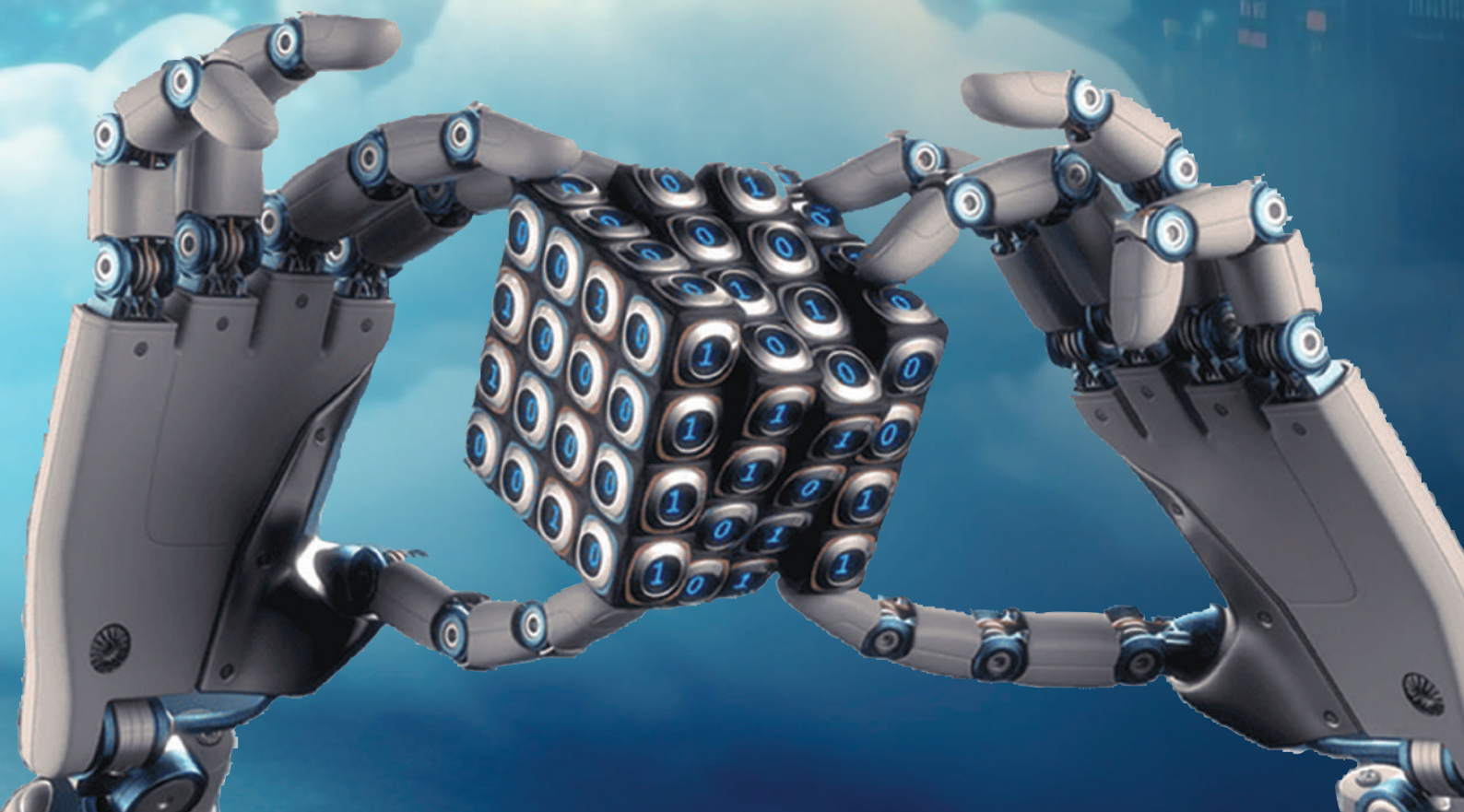
Основными потребителями нашей продукции являются корпоративные и коммерческие ЦОДы, ритейловые компании, крупные банки, ведущие транспортные, энергетические и нефтегазовые компании, спортивные объекты, а также офисные и выставочные комплексы.

Мы готовы к новым крупным проектам и интересным вызовам рынка, всегда открыты для предложений и запросов.

Российские облака – 2022: интеграция и конвергенция

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

Отечественный облачный рынок, на котором набирает популярность облачная интеграция, подходит к этапу консолидации. Еще один тренд – конвергенция информационных и операционных технологий – создает как вызовы, так и возможности для игроков рынка.



Смена стратегий

За минувший год многие провайдеры кардинально изменили свои стратегии. Если в начале 2022 г. все пытались удовлетворить растущий спрос на отечественные облака, то ближе к лету стали задумываться о стратегии. Одни поставили во главу угла замещение софтверного стека для себя, другие налаживали каналы параллельного импорта оборудования, о чем я писал в первой части статьи*. Третьи пытались решить проблемы с ПО для клиентов, начиная предлагать в рамках своих услуг лицензии на отечественное ПО или переходить к концепции bring your own license. Если клиент обладал, например, лицензиями ПО Microsoft, то он мог арендовать у провайдера облачную инфраструктуру, загрузить ISO-образ диска и инсталлировать привычную ему Windows на виртуальную машину. Юридически тут всё чисто, лицензия не нарушается ни провайдером, ни клиентом. Но для того чтобы это сделать, нужно доработать провайдерские панели управления облаком – у многих такой возможности просто нет.

Некоторые провайдеры задумались о геоэкспансии. Кто-то купил ЦОД в Беларуси у уходящего игрока, кто-то стал отказываться от европейских ЦОДов и открывать новые площадки на южном направлении: в Средней Азии, в Израиле или ОАЭ – «теперь не Франкфурт, а Дубай, но сервис от этого не меняется».

Резервная площадка в другой стране – понятная стратегия, на такое решение есть стабильный нишевый спрос. Однако те ограничения, с которыми столкнулись отечественные клиенты в плане доступа к зарубежному ПО, породили новые подходы: от лобовых попыток предоставлять трансграничный сервис на базе SAP или Microsoft с использованием провайдерских лицензий до более изобретательных – отдавать виртуальные десктопы с тем же привычным десктопным ПО, которое нынче недоступно. И тут можно использовать хоть 3D-редакторы, хоть CAD. Все это «серая» зона, но и она нашла свой спрос, пусть не слишком масштабируемый и сопряженный с риском.

Производная второго порядка от этого тренда – стремление к разделению бизнеса. Ряд провайдеров из топ-10, которые уже имели зарубежные площадки и иностранных клиентов и добились успеха за рубежом, решили провести финансовое, инфраструктурное, командное и организационное разделение бизнеса. При этом чаще всего подразделение R&D остается общим для де-факто независимых компаний. Но ничего нового в этом нет, многие глобальные софтверные вендоры с корнями из РФ – Abbyy, Acronis и др. – так поступили существенно раньше.

Ряд других российских облачных провайдеров сейчас «упаковывается» к продаже. Сокращение «кормовой базы» вследствие ухода иностранных компаний даже при перспективах повышения внутреннего спроса в условиях ограничения конкуренции со стороны глобальных гиперскейлеров – всё это расценивается как стратегический риск. А поскольку бизнес очень хорошо поднялся в 2022 г. и рынок, согласно прогнозам аналитиков, продолжает расти двузначными темпами, момент для продажи самый что ни на есть удачный. А значит, будут укрупнение и консолидация. В западном мире они уже произошли. Сейчас у американских предприятий выбор, в какое облако пойти, невелик: AWS, Azure, GCP или IBM. Аналогичная картина будет через несколько лет и у нас. Но у российских компаний на вопрос, какое облако выбрать, варианты ответов будут другими: операторское, банковское, «промышленно-энергетическое» или облака «гиперскейлеров-поисковиков». Если взглянуть на топ-10 провайдеров по долям рынка, то тенденции хорошо считываются. Да, на рынке есть интеграторы и независимые игроки, но это пока. Все они либо продадут бизнес, либо переквалифицируются в облачные интеграторы.

Облачная интеграция

Давайте разберемся, что же это за модель «облачная интеграция», которая на нашем рынке делается все популярнее.

Классическая системная интеграция – это процесс объединения различных систем, приложений и технологий в целостную инфраструктуру, позволяющую эффективно управлять бизнес-процессами и повышать производительность предприятия. Современные технологии, такие как искусственный интеллект, облака и промышленный интернет вещей, существенно меняют подходы к системной интеграции и расширяют ее возможности.

Облачный системный интегратор – это по сути то, что на Западе называлось Managed Service Provider (MSP), и доля рынка у таких игроков еще 10 лет назад была довольно весомой. MSP сочетал предоставление облачных инфраструктурных, аналитических, сетевых услуг (IaaS/AaaS/NaaS), услуг консалтинга и классической системной интеграции. Он собирал для клиента решение под ключ с минимальной долей самообслуживания или даже без него. MSP мог иметь свой ЦОД либо свое облако в коммерческом ЦОДе или же, как чаще всего происходит теперь, оказывать услуги на базе инфраструктуры одного из глобальных гиперскейлеров. Подобная компания по запросу клиента

* Салов А. Российские облака: уроки 2022 года // «ИКС» № 2'2023, с. 61.

объединяет в единую инфраструктуру облачные сервисы и приложения разных поставщиков, а также предоставляет управление, мониторинг и техническую поддержку этой инфраструктуры. Основная идея заключается в том, чтобы упростить процесс внедрения и применения облачных решений для клиентов. Обычно при использовании облачных сервисов клиенты сталкиваются с необходимостью управлять несколькими аккаунтами, сервисами и приложениями, что может быть сложно и трудоемко. Хорошо работающий мультиклауд построить тяжело. Облачный интегратор объединяет все сервисы в единую инфраструктуру и обеспечивает возможность управлять ею через один интерфейс.

Кроме того, облачный интегратор может предоставлять дополнительные сервисы: мониторинг производительности, резервное копирование, безопасность и техническую поддержку. Эти сервисы позволяют клиентам сосредоточиться на своем бизнесе, а не на управлении ИТ-инфраструктурой. Облачные интеграторы могут быть полезны как для крупных корпораций, так и для малых и средних предприятий, которые не имеют достаточных ресурсов для создания собственной ИТ-инфраструктуры.

В России идет аналогичный процесс – многие системные интеграторы сначала обзавелись собственными ЦОДами, развернули свои облака и даже заняли серьезную долю рынка. Но потом под давлением ряда рыночных факторов они начали либо выделять из бизнеса и продавать облачные подразделения, либо вступать в партнерства с гиперскейлерами, переводя клиентов на их инфраструктуру.

Останется ли в пищевой цепочке место для системной интеграции? Да, конечно. Просто области применения и компетенции должны измениться. Основные векторы приложения усилий – это облака, искусственный интеллект и промышленный интернет вещей.

Как уже было отмечено, облачные технологии сильно влияют на будущее системной интеграции. Многие системные интеграторы сфокусировались на том, чтобы собирать в соответствии с требованиями клиента импортозамещающий стек – от серверов до программного обеспечения. Заместить импортную ИТ-инфраструктуру отечественной – задача нетривиальная. Выбор решений широкий, однако совместимость компонентов под большим вопросом. Провести тестирование и добиться гарантированной работы элементов даже крупному корпоративному клиенту зачастую не под силу. А интегратор, собрав рабочую конфигурацию, разворачивает ее в облаке и отвечает за доступность и надежность системы, репликацию данных и мониторинг состояния серверов.

Искусственный интеллект (ИИ) также играет важную роль в будущем системной интеграции. ИИ может использоваться для автоматического обнаружения проблем (например, в вопросах кибербезопасности) и нахождения эффективных решений. Это поможет улучшить процессы мониторинга и управления, сократить время реакции на проблемы и уменьшить количество ошибок. Кроме того, ИИ может обеспечить анализ большого объема данных и предоставить ценную информацию для принятия управленческих решений. Спрос на решения на базе ИИ растет, но такие системы требуют серьезных вычислительных ресурсов и компетенций, которые может предоставить профильный интегратор.

Еще один фактор влияния на будущее системной интеграции – промышленный интернет вещей (IIoT). Фокус государства на росте промышленного сектора, ввод новых фабрик и заводов на территории РФ обуславливает рост спроса на промышленную автоматизацию. IIoT позволяет устройствам собирать и передавать данные о своем состоянии и работе в реальном времени. Это может быть полезно для мониторинга обору-

дования и автоматического оповещения о поломках или сбоях в работе. Предиктивная аналитика на базе технологий IIoT улучшит автоматизацию производственных процессов и повысит их эффективность. IIoT порождает массивы информации, которые надо собирать в озера данных. Они, в свою очередь, требуют построения edge- или частных облаков в контуре предприятия, а это – отдельные компетенции.

Конвергенция ИТ и ОТ

Облака как явный тренд информационных технологий последних 15 лет серьезно трансформировали подход к созданию вычислительной инфраструктуры. Перенос основных офисных процессов из серверных в ЦОДы позволил обеспечить непрерывность работы, несмотря на экспоненциальный рост данных и тектонические сдвиги, к которым можно отнести пандемию. Многие компании вернулись с «удаленки», но сохранили гибридный график работы для своих сотрудников. Он дает существенную экономию на аренде площадей и инфраструктуре – гибкие рабочие места в офисе, работа домашнего ПК сотрудника. И там и там безопасность данных обеспечивает инфраструктура виртуальных рабочих столов, развернутая в облаке. Электронная почта, телефония, ВКС, CRM, ERP, разработка ПО – всё это мигрировало в облако. ИТ стали облачными – где-то больше (в изначально цифровых компаниях и стартапах), где-то меньше (например, в банках – в силу регуляторных ограничений).

Однако, если мы покинем уютный офис и перейдем в реальный сектор экономики, то обнаружим, что проникновение облаков там существенно ниже. В агросекторе это объясняется ограничением каналов связи (многие фермерские хозяйства находятся вне зоны стабильного покрытия LTE, а о выделенных каналах связи им остается только мечтать), но на непрерывном или дискретном производстве недоверие к облакам связано с критичностью процессов, управление которыми нельзя вынести в централизованный дата-центр к внешнему провайдеру. Здесь и вопрос безопасности данных, и критичность задержек для SCADA.

В то же время цифровизация производства идет полным ходом. Эффективно управлять процессами на современном предприятии без внедрения операционных технологий (ОТ) нельзя. Контроль состояния турбин, мониторинг прокатных станов, роботизация, производственная безопасность, логистика «от поля до прилавка» – всё это оцифровывается каждый день. Развитие отечественного производства поддерживается на государственном уровне, финансовые потоки направляются в реальный сектор экономики. Уже и руководство страны говорит о том, что нужно переходить от регламентного ремонта к ремонту по состоянию, а это означает внедрение предиктивной диагностики и аналитики, создание цифровых двойников производства.

На стыке информационных и операционных технологий рождается новый тренд, который будет определять развитие облаков в ближайшее время. Этот тренд – ИТ/ОТ-конвергенция, т.е. объединение и взаимопроникновение технологий и процессов. Грань между ИТ и ОТ иногда может быть размытой, разница между ними сводится к тому, как эти технологии используются.

ИТ обычно сосредоточены на сборе и обработке информации, которая может использоваться компаниями для управления бизнес-процессами или анализа. ОТ обычно ориентированы на сбор и обработку информации для управления станками или другим оборудованием, задействованным в физических процессах.

В прошлом ИТ ассоциировались с офисами и работой «белых воротничков», тогда как ОТ связывались с фабриками, складами, доставкой и работой «синих воротничков». Сегодня компании все чаще хотят согласовать эти различные виды работы друг с другом, и это одна из причин, по которой они хотят подключить свои ИТ-системы к ОТ-системам. В последние годы стали доступны большие вычислительные мощности, улучшенные сети, более емкие и быстрые

хранилища и новые технологии IoT, которые позволяют OT и ИТ-системам легко обмениваться данными друг с другом.

Например, возможность собирать, обрабатывать и анализировать данные из OT-систем позволяет компаниям лучше использовать свои ИТ-системы для оптимизации бизнес-процессов и получения информации, которая может послужить для стимулирования инноваций или внедрения новых услуг. Вместе с тем благодаря системам OT, которые можно обновлять или оптимизировать с помощью данных из ИТ-систем, компании могут улучшить управление различными физическими операциями.

Производственники все еще неохотно передают данные за периметр организации, а значит, вычисления надо переносить внутрь этого периметра, но иметь возможность ими удаленно управлять. Здесь нам на помощь приходят edge-вычисления, т.е. обработка данных в непосредственной близости от их источника, что позволяет уменьшить задержку при обработке и снизить нагрузку на центральные облачные серверы. Edge-вычисления дают возможность выполнять критические операции с минимальными задержками, гибко настраивать безопасность данных, экономить на каналах связи и при этом пользоваться всеми преимуществами больших вычислительных облаков, передавая туда предобработанную информацию, которая необходима для глубокого анализа. Повышение безопасности и конфиденциальности данных крайне важно в OT. Edge-вычисления помогут снизить риски потери данных, поскольку данные можно обрабатывать и сохранять на месте без передачи по сети на центральные облачные серверы.

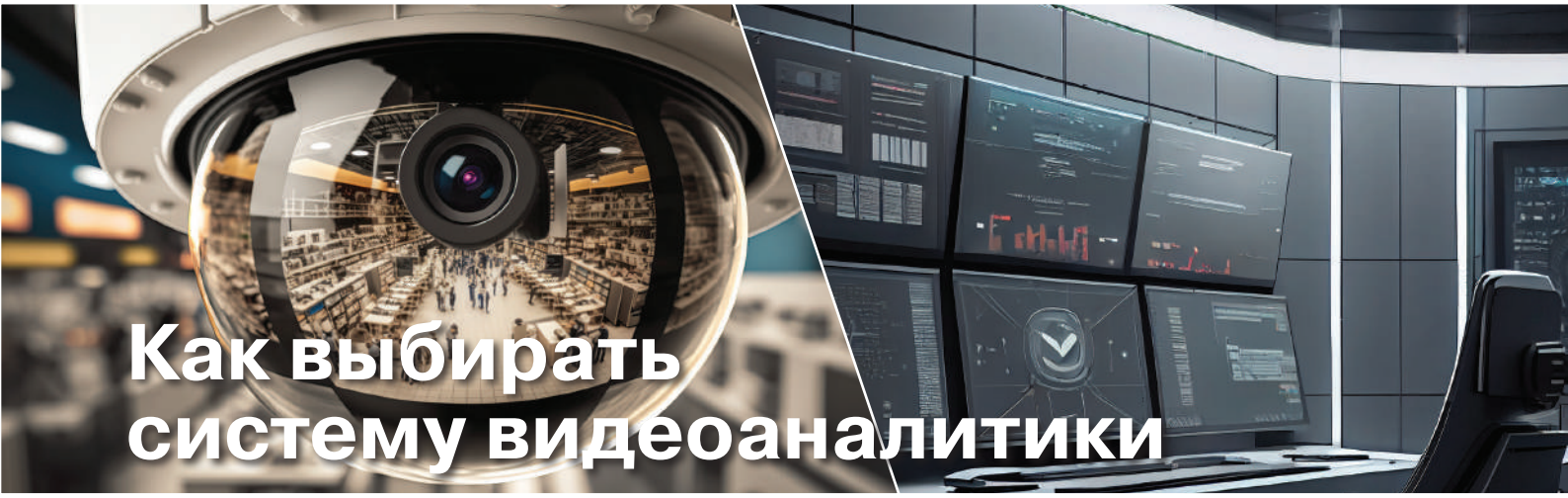
Облачные провайдеры также делятся на тех, кто сосредоточился исключительно на облаках для ИТ-процессов, и на тех, кто уже активно идет в ИТ/OT-конвергенцию. К первой группе можно отнести наших гиперскейлеров, ко второй – операторов связи и интеграторов с собственными облаками. Это логично, у операторов есть бизнес по строительству частных сетей LTE с edge-нодами, и они научились зарабатывать на IoT/IIoT, а интеграторы изначально выполняют комплексные проекты автоматизации производства.

Ставка на сбор и анализ информации, поступающей с IoT-датчиков, может дать преимущество, так как число датчиков растет в геометрической прогрессии по мере удешевления, и с большой вероятностью данные для дальнейшей обработки не отдадут в ЦОД гиперскейлера. Например, МТС предоставляет сервис облачной АСКУЭ (автоматизированной системы коммерческого учета электроэнергии). Это по сути та же CRM, но специализированная, ориентированная на отраслевые процессы энергосбытовых компаний. Ее обязательное внедрение регламентировано федеральным законодательством. Данные, которые собираются с «умных» приборов учета (ПУ), накапливаются в АСКУЭ, и на основе анализа этих данных формируется новая услуга – поиск потерь из-за взломанных ПУ. Вот ИТ/OT-конвергенция, которая уже работает.

Этот тренд окажет влияние и на региональную экспансию ЦОДов: по мере развития производственных кластеров рядом с ними будут появляться и ЦОДы для обеспечения потребностей в вычислениях. Конвергенция OT и ИТ приводит к увеличению количества устройств, подключенных к сети, а также к увеличению объемов данных, которые необходимо обрабатывать и хранить. В связи с этим спрос на услуги региональных ЦОДов будет увеличиваться, поскольку производственники будут нуждаться в большей мощности вычислений и хранения данных. Этим обусловлено появление провайдеров услуг ЦОДов и облаков при крупных промышленных и энергетических холдингах.

Однако конвергенция OT и ИТ заставит предъявлять к региональным ЦОДам более высокие требования. Например, данные, собранные из OT-систем, могут быть критически важными для бизнеса, и их потеря или недоступность могут иметь серьезные последствия. Поэтому операторам региональных и edge-ЦОДов придется должным образом обеспечивать защиту данных и бесперебойность своих услуг.

Таким образом, усиление конвергенции OT и ИТ создает как вызовы, так и возможности для рынка региональных ЦОДов в России. Компании, которые смогут адаптироваться к этим изменениям и предоставить высококачественные услуги, будут иметь больше шансов на успех. ИКС



Как выбирать систему видеоаналитики

ИТ-рынок предлагает множество систем видеоаналитики, поэтому сделать выбор непросто, особенно если компания не обладает необходимой экспертизой. На что нужно обратить внимание, чтобы приобретенная система работала долго и эффективно?

Иван Корсаков, архитектор систем компьютерного зрения, Softline Digital

Какая именно система нужна?

Системы видеоаналитики применяются в разных областях: в сфере обеспечения безопасности, на транспорте, в розничной торговле, промышленности и т.д. С точки зрения сложности их можно разделить на несколько категорий.

- Системы, способные выполнять простой анализ видео. Например, они осуществляют детекцию движения или распознавание государственных регистрационных знаков на транспортных средствах без дополнительного анализа. Детекция движения помогает отслеживать движущиеся объекты, что может быть полезно для обнаружения несанкционированных действий или контроля перемещений в определенной области. Распознавание номерных знаков обеспечивает обработку видеоданных, связанных с движением транспортных средств, их классификацией и анализом трафика.
- Среднесложная система видеоаналитики способна выдать оповещение/сигнал тревоги в случае происшествия либо при обнаружении, скажем, пожара или дыма. Это позволяет оперативно реагировать на возгорание. Еще один пример – системы распознавания лиц с поиском по предварительно сформированным группам и спискам. Они могут использоваться в системах безопасности, СКУД, при поиске пропавших людей и т.д.
- Комплексные системы видеоаналитики на крупных предприятиях решают гораздо более серьезные задачи. Часто такие системы интегрируются в сложные производственные процессы. Так, в системе учета трубной продукции задействуются несколько десятков камер, начиная с машины для центробежного литья, печей для отжига и заканчивая установками дефектоскопии труб. На каждом этапе проводится учет труб надлежащего качества и выявление некачественных, классификация по диаметру, дефектоскопия и многое другое. Эта же система решает задачи обеспечения промышленной безопасности, охраны периметра и т.д. Она выдает готовые отчеты и уведомления для ответственных лиц согласно принятым на производстве нормативным документам.

Компания должна четко понимать, для каких целей и задач на предприятии нужна видеоаналитика.

«Коробка» или кастомизированная разработка?

Некоторые компании убеждены, что внедрение системы видеоаналитики в производственный процесс всегда требует индивидуальной (кастомизированной) разработки с нуля. Это не так. Во многих случаях достаточно готового коробочного решения. Однако нужно понимать различия между коробочным решением и кастомизированной разработкой.

Коробочные решения выполняют конкретные задачи в заранее определенных технических условиях наблюдения. Поэтому прежде всего нужно оценить их применимость в условиях заказчика. Для этого необходимо провести технический аудит. Кроме того, интеграция этих систем в производственные процессы и их настройка в соответствии с особенностями того или иного предприятия могут потребовать доработки.

Наиболее привлекательным вариантом может стать высококачественная коробочная система, которая требует минимальной адаптации к специфике заказчика. Кроме легкости интеграции и

использования, современные коробочные решения экономят время: систему можно быстро протестировать и оценить ее эффективность.

Однако при покупке коробочного продукта нужно понимать, что на ИТ-рынке есть недобросовестные поставщики услуг. Такие компании предоставляют клиентам систему видеоаналитики, которая якобы базируется на уже готовых нейросетях, а затем берут дополнительную плату за доработку решения или обучение нейросети, хотя на самом деле осуществляют разработку с нуля. Также, заявляя о работоспособности своего решения, они могут опускать тот факт, что условия его эксплуатации должны быть намного «стерильнее», чем на объекте заказчика.

Несколько иначе выглядит ситуация со сложными комплексными системами, такими как системы дефектоскопии, системами «все в одном», которые решают сразу много задач из разных областей. Лучший вариант здесь – проектирование системы в соответствии с нуждами заказчика. Это предполагает объединение отдельных компонентов и алгоритмов в единую уникальную для каждого проекта систему с анализом их потенциала применимости, интеграции друг с другом и масштабирования.

Так, по запросу клиента можно собрать систему видеоаналитики, которая будет распознавать, носят ли рабочие каски и спецодежду на производстве, обнаруживать людей в инфракрасном диапазоне для задач охраны, выявлять утечки масла, а также огонь и дым на открытом складе. Такие сценарии существуют поодиночке, но при создании комплексной системы могут нуждаться в интеграции друг с другом.

Важно понять, были ли подобные решения разработаны для конкретных задач или они могут быть адаптированы для применения в разных сферах. Например, алгоритм видеоаналитики, созданный для дефектоскопии колодок, имеет узкие границы применимости и, возможно, даже не существует как законченная система, однако может быть интегрирован в комплексную систему видеоаналитики, разрабатываемую для большой задачи, частью которой является дефектоскопия колодок. Для того чтобы понять, действительно ли необходимо разрабатывать новое решение или можно модернизировать существующее, также необходим технический аудит.

Подводные камни кастомизированного решения

Если же готового решения для необходимого сценария на рынке нет, остается вариант с индивидуальной разработкой. В этом случае нужно со всем вниманием отнестись к составлению технического задания. Важнейший момент – определять не конкретные камеры, а технические условия, в которых должна функционировать система. Иначе заказчик получит систему, формально соответствующую техническому заданию по всем пунктам, но совершенно не выполняющую поставленную бизнес-задачу.

Например, система видеоаналитики успешно внедрена и прошла пилотный запуск, все акты подписаны. Однако при добавлении еще пяти камер она начинает выдавать большое количество ложных срабатываний, хотя с первоначальными камерами работала безупречно. Дело в том, что для полноценного обучения системы нужен большой объем данных, который включает в себя множество изображений с разных камер. Только обученные должным образом системы видеоаналитики работают без привязки к конкретному оборудованию. Если же поставщик сэкономил на ресурсах и обучил систему работать только с конкретным расположением камер, что намного проще, то результат будет неудовлетворительным.

Избежать этого можно путем фиксации в ТЗ технических условий. Безусловно, после этого заказчику придется соблюдать определенные стандарты освещенности, углов поворота камер, размеров объектов, видимости и контрастности. Но только так можно гарантировать точность работы системы распознавания не ниже определенного уровня.

Но даже соблюдение всех рекомендаций не гарантирует продолжение работы системы на должном уровне, например, при изменении бизнес-процессов. Если же такое изменение планируется, то соответствующие требования также должны быть отражены в ТЗ.

Если нужно добавить в систему камеры, есть два варианта действий:

- соблюсти существующие технические условия при размещении новых камер;
- обратиться к поставщику решения для доработки и дополнительного обучения системы.

Возможность добавления новых камер на начальном этапе часто не принимают во внимание. В результате сложно оценить полную стоимость системы – не в рамках пилотного проекта с 5–10 камерами, а в реальных условиях эксплуатации, когда система масштабируется и требует поддержки. Некоторые подрядчики могут развернуть систему из 5–10 камер недорого, но установка следующих 5–10 камер обойдется примерно в такую же сумму, тогда как стоимость масштабирования правильно спроектированной системы всегда существенно ниже.

Каким должен быть процесс выбора системы?

Системы видеоаналитики представляют собой сложные инженерные системы. Их выбор требу-

ет специальной экспертизы, которой у большинства ИТ-департаментов предприятий нет.

На первом этапе нужно изучить рынок и во взаимодействии с потенциальными поставщиками получить представление о том, что они предлагают. Преимущество следует отдавать тем компаниям, которые готовы оперативно пилотировать свои системы на конкретных производственных площадках заказчика.

При проведении тендера следует учесть, что техническая компетентность участников, как правило, высока и обязательное условие для победы – успешная реализация пилотного проекта. В этом контексте пилотный проект предполагает использование уже функционирующих на предприятии камер.

При использовании 10–15 камер оптимальный срок для установки и тестирования системы – одна-две недели. Заказчик предоставляет сервер, а ИТ-специалисты выделяют два-три дня на развертывание решения, которое затем тестируется в течение 5–10 дней. Если же у поставщика нет наработок или готового решения, он, скорее всего, не сможет в такой срок продемонстрировать результат, поскольку не успеет внести в систему изменения для учета специфики камер заказчика.

Чтобы избежать получения решения, которое формально соответствует техническому заданию, но на практике не работает, следует детально прописать в ТЗ все нюансы, включая показатели качества работы системы и процесс ее приемки. К примеру, если компания заказывает систему для распознавания номеров вагонов, в ТЗ должен быть предусмотрен протокол, который фиксирует фактическое количество номеров на поезде, количество распознанных номеров и процент успешного распознавания в разное время суток при разных погодных условиях.

Не проводить тестирование на основе видео!

При проведении тестирования заказчики часто совершают серьезную ошибку – вместо полноценного тестирования на «живых» видеопотоках передают поставщику готовое видео и оценивают работу системы исключительно по прямоугольникам, которые система рисует на видео для тех или иных событий.

Здесь возможны две проблемы. Первая заключается в том, что поставщик может попросту отредактировать видео так, как ему необходимо, чтобы показать идеальный результат.

Кроме того, видео может быть использовано для обучения новой нейронной сети, которая работает только с этим конкретным видеоматериалом. Заказчику же сообщат, что сеть работает, и он увидит, что она действительно функционирует, но при интеграции системы потребуются значительная доработка и обучение.

Скажем, система функционирует с одной камерой или несколькими камерами с определенными техническими условиями видеонаблюдения. Затем нужно добавить еще десять камер, но с другими характеристиками. И соответственно под каждую потребуется обучать систему.

Вторая проблема – в непонимании сути работы видеоаналитики. Результат работы системы видеоаналитики – это не прямоугольники красного и зеленого цвета, а отчеты и статистика, а также уведомления и управляющие сигналы для различных устройств. Таким образом, ролик, на котором видно, что система определяет нужное событие, не является показательным, потому что по нему непонятно, сколько таких инцидентов она пропускает, сколько у нее ложных срабатываний, сколько уведомлений на одно событие она генерирует.

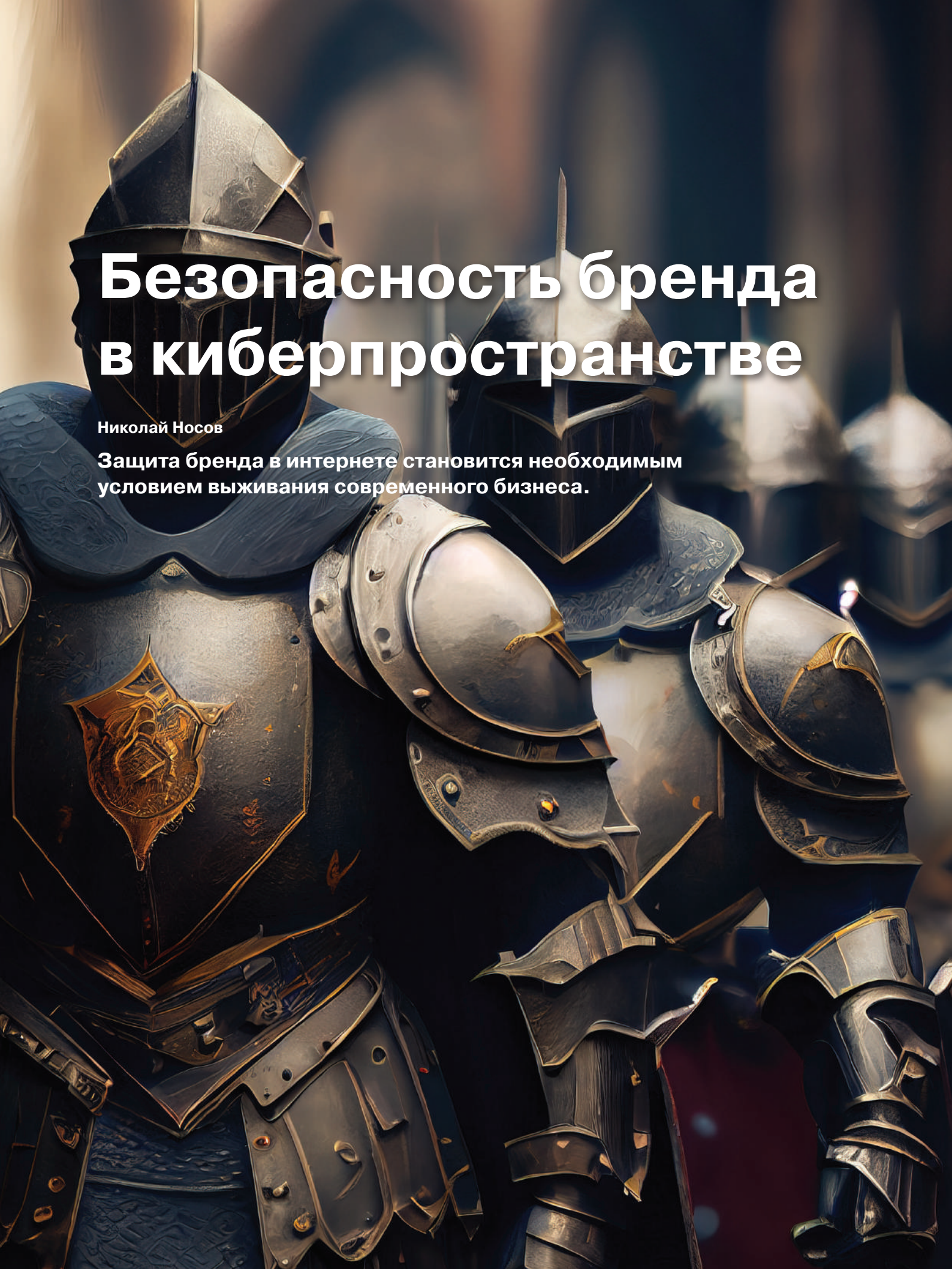
К примеру, автор видел установленную систему определения нарушений ОТиПБ, которая работала и действительно выявляла инциденты с нарушением техники безопасности. На представленных видеороликах система работала идеально, все события обводились красивой красной рамкой. Однако при введении в эксплуатацию выяснилось, что вместо одного фактического события с нарушением ОТиПБ система выдавала события каждую секунду, а также имела высокий процент ложных срабатываний. В итоге системой просто не пользуются, поскольку просмотр всех событий в ней занимает больше времени, чем просмотр камер без видеоаналитики.

При тестировании же на видеокамерах заказчика установленная система может немедленно предоставлять необходимую информацию и сразу будет ясно, насколько можно ей доверять, насколько удобно использовать ее отчеты, насколько сильно она ошибается.

Тестирование по видео не позволяет достоверно оценить способность системы работать с разными камерами. Поэтому особое внимание следует уделять системам, готовым к развертыванию в контуре заказчика. Внедрение таких систем позволит существенно сократить затраты на цифровизацию и легче масштабировать решение.

■■■

Чтобы избежать риска, что подрядчик не справится с задачей или справится формально, так что использовать систему будет невозможно, нужно четко сформулировать условия приемки системы и согласовать их на ранних этапах проекта. Важно, чтобы исполнитель и заказчик имели общую цель – создать систему, которая будет эффективной, приносить пользу и в конечном счете окупится. ИКС



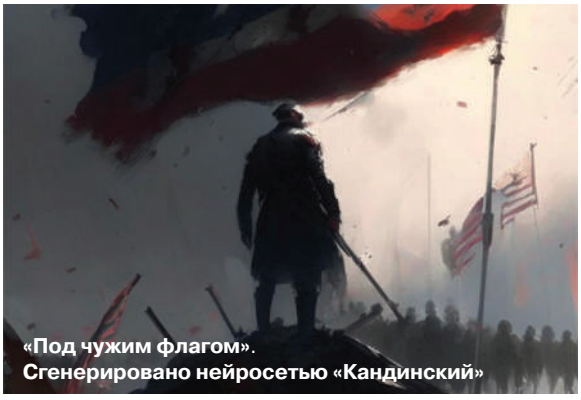
Безопасность бренда в киберпространстве

Николай Носов

Защита бренда в интернете становится необходимым условием выживания современного бизнеса.

Под чужим флагом

В конце 2022 г. неизвестный создал поддельный Twitter-аккаунт фармацевтической компании Eli Lilly и опубликовал пост: «Мы рады сообщить, что инсулин теперь бесплатный». Пользователи не распознали фальшивку – у сообщения стояла голубая галочка, подтверждающая подлинность. Как потом выяснилось, за $8 ее мог купить кто угодно. Началась паника, от акций компании стали стремительно избавляться. По разным источникам, за пару часов фармгигант потерял $6,8–16 млрд рыночной стоимости – вот наглядный пример необходимости защиты бренда в киберпространстве. Под чужим флагом могли выступить активисты, возмущенные тем, что с 1996 г. инсулин подорожал на 1200%, или конкуренты, хотя они тоже пострадали, правда, в меньшей степени.



«Под чужим флагом». Сгенерировано нейросетью «Кандинский»

В современном мире нематериальные активы составляют основную часть стоимости компании. «Раньше рыночная стоимость компании определялась тремя-пятью ее годовыми оборотами, а деньги, вложенные в акции, можно было вернуть за счет дивидендов. Сейчас акции покупают из-за привлекательности компании – это цена надежды. Высокая стоимость определяется надеждой, и она очень уязвима. Поэтому репутационные атаки – это удар по основам бизнеса. Например, победить конкурента в тендере проще, подсунув на него компромат, чем в честной борьбе», – дал комментарий нашему изданию президент консорциума «Инфорус» Андрей Масалович.

Здоровье бренда

Киберпространство существенно влияет на восприятие бренда, или, выражаясь языком маркетологов, на его «здоровье». Раньше доверие к бренду определялось путем опросов. Теперь же, как объяснила директор отдела по анализу социальных медиа Ipsos Полина Жигарева, можно анализировать открытые источники в интернете, включая блоги, форумы, чаты, мессенджеры и социальные сети, и использовать индексы доверия, пришедшие из политических исследований.

Так, по результатам анализа социальных медиа рассчитывается принимающий значения от -1 (полное недоверие) до +1 (полное доверие) индекс BSG Trust, который учитывает параметры «компетентность» (может ли компания выполнить поставленную задачу), «прозрачность» (насколько открыты и однозначны ее решения), «справедливость» (насколько компания выполняет обещания), «устойчивость» (насколько эффективно компания избегает кризисов и восстанавливается после них). Программные средства для подобного анализа имеет, например, понимающая даже сленг и тон сообщений в Сети система компании Brand Analytics.

Для повышения доверия к бренду в киберпространстве могут привлекаться пиар-агенства, применяющие разнообразные инструменты: от проведения массовых рекламных кампаний до «накрутки» с помощью ботов положительных отзывов на сайтах-отзовиках. Улучшить здоровье своего бренда можно, ухудшив здоровье брендов-конкурентов. К этим средствам прибегают нечистоплотные компании, заказывающие «черный» пиар и развязывающие информационные войны. Среди возможных векторов атак: дискредитация бренда с помощью специально подготовленных скандалов и провокаций; негативные отзывы о бренде в чатах, форумах, социальных сетях; кража, т.е. использование вашего бренда конкурентом, а еще хуже – мошенником, создающим фишинговый сайт.

Основные этапы противодействия – мониторинг с целью раннего выявления угроз, анализ ситуации и прогноз развития атаки на бренд, выработка адекватных ответных мер и оценка рисков.

Управление репутацией

Одними из первых на защиту бренда в интернете встали пиар-агентства, имеющие большой опыт управления репутацией политиков в офлайне и рано осознавшие угрозы для бренда, таящиеся в Сети. Накопленный опыт стали применять для управления репутацией компаний. Характерный пример – компания «Сидорин

> Защита бренда и репутации важны для любого бизнеса, но более всего для компаний, у которых репутация напрямую влияет на привлекательность для покупателя. Прежде всего это розница и традиционный банковский бизнес. Также стоит упомянуть телеком, ИТ- и ИБ-компании, которым важно доверие клиентов, а доверие ассоциируется с брендом.

Анна Кулашова, управляющий директор в РФ и СНГ, «Лаборатория Касперского»

Лаб», основатель которой Дмитрий Сидорин работал на выборах президента РФ в штабе кандидата Михаила Прохорова. Сейчас его агентство – один из основных игроков рынка защиты бренда. Среди других агентств, занимающих заметные позиции на рынке защиты репутации, можно назвать Faros.Media, K-Reputation, MarkWay, Rush Agency, Topface Media, uForce и «Интериум».

Рынок управления онлайн-репутацией шире, чем рынок защиты бренда, поскольку включает в себя инструменты и услуги создания имиджа: онлайн-пиар, оптимизацию поисковой выдачи, анализ репутации, управление отзывами и рейтингами. По данным исследования TMT Consulting, в 2020 г. рынок управления онлайн-репутацией в России составил примерно 1,7 млрд руб. Сумма включает в себя доходы от услуг мониторинга, анализа и управления онлайн-репутацией компаний и частных лиц.

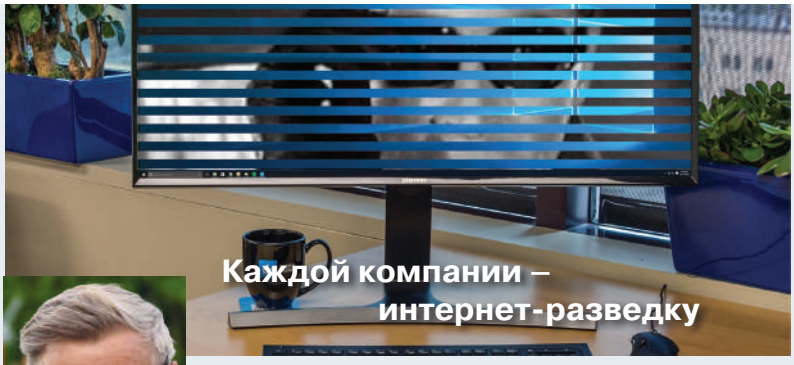
По оценке «Сидорин Лаб», за последние три года эта цифра выросла еще минимум на 10%, будет продолжать расти и в 2025 г. достигнет 2 млрд руб. Драйверами станут увеличение числа интернет-пользователей и развитие сетей и платформ для обмена отзывами. Компании будут активнее мониторить интернет и реагировать на обсуждение своих продуктов и услуг в онлайн-среде.

Защита от киберпреступников

Бренд может пострадать не только в результате информационных войн, но и из-за действий киберпреступников. Мошенники создают фишинговые сайты, использующие цвета бренда и логотипы компании, для кражи паролей, номеров банковских карт и других персональных данных. Иногда фейковые сайты создают для обмана пользователей: «продавая» товары, собирая деньги по случаю резонансных событий или проводя розыгрыши несуществующих лотерей.

Сильно бьют по репутации реальные или фиктивные утечки данных, о которых все чаще сообщают СМИ. По оценке McKinsey & Company, 71% потребителей откажется от услуг компании, без разрешения разглашающей конфиденциальные данные клиентов.

Неудивительно, что к защите бренда подключились компании, работающие в сфере кибербезопасности. В отличие от пиар-агенств, занимающихся как созданием брендов, так и их защитой, специалисты по информационной безопасности сосредоточиваются прежде всего на защите. Причем если зарубежные компании под термином «защита бренда» (Brand Protection) подразумевают узкую нишу защиты бренда от неправомочного использования и контрафакта, то на российском рынке – защиту бренда от всех угроз в киберпространстве, что на Западе описывают зонтичным термином «защита от



Каждой компании – интернет-разведку

Андрей Масалович, президент, «Инфорус», преподаватель по OSINT, «Безопасность 360»

Именитые бренды неизбежно становятся участниками информационной войны и все время находятся под ударом. Первый вектор атаки – дискредитация бренда. Это продуманная целевая атака по болевым точкам, скандалы и провокации. Второй вектор – кража бренда и контрафакт. Под вашей маркой конкуренты могут выпускать свою, зачастую некачественную продукцию. Третий – размещение в интернете негативных отзывов недовольными бывшими сотрудниками, конкурентами и просто недоброжелателями. Такие отзывы – необязательно целевая атака, но они тоже бьют по репутации бренда.

Противодействие атакам на бренд в информационном пространстве можно разбить на три этапа. Первый и очень важный – мониторинг и раннее предупреждение. Информационные атаки можно нейтрализовать, но их надо вовремя обнаруживать. Если время упущено – реагирование станет очень дорогим, если не невозможным.

Второй этап – анализ и интерпретация ситуации: кто напал, каков возможный бюджет, чего стоит ждать.

Третий – собственно ответные действия. Важно, что действия должны быть адекватными, так как реагировать неадекватно – хуже, чем не делать ничего.

Контроль обстановки, раннее обнаружение, быстрое реагирование – вот задачи, которые решает интернет-разведка по открытым источникам (open source intelligence, OSINT). Отдельные направления OSINT тесно примыкают к теме защиты бренда. Первым в России это понял Герман Греф, еще восемь лет назад выпустивший распоряжение по Сбербанку о передаче мониторинга устойчивости бренда от пиар-службы службе экономической безопасности.

Основные шаги по противодействию атакам на бренд:

- очистить информацию, удалить мусор и фейки;
- раскрасить информацию, выделить важную, требующую реакции;

цифровых рисков» (Digital Risk Protection, DRP), а Brand Protection рассматривают как одно из направлений DRP.

В число направлений DRP, согласно западной таксономии, входят:

- мониторинг доменов (Domain Monitoring);
- предотвращение перехвата учетных записей (Account Takeover Prevention);
- защита в соцсетях, в том числе выявление фейков, поддельных аккаунтов, информационных атак (Social Media Protection);
- защита бренда (Brand Protection);
- мониторинг утечек (Data Leak Detection);
- защита первых лиц (Executive Protection).

Для разных сценариев используются разные инструменты, но на практике чаще всего они объединяются в один DRP-продукт, предлагаемый заказчику по сервисной модели.

Мировые лидеры

Согласно отчету Global Digital Risk Protection Software Industry Research Report 2023, опубликованному аналитическим агентством Absolute Reports, объем мирового рынка программного обеспечения DRP составил в 2022 г. $2908,42 млн. Ожидается, что он будет увеличиваться ежегодно в среднем на 13% и к 2028 г. достигнет $6083,75 млн.

Ведущие позиции на мировом рынке занимают компании PhishLabs (платформа Forta); DigitalStakeout, разработавшая одну из лучших систем мониторинга даркнета; RiskIQ, купленная Microsoft (решение Microsoft Defender); Digital Shadows (решение ReliaQuest); помогающие управлять репутацией американские Cyberint и ZeroFox.

> Рост числа фишинговых страниц связан во многом с автоматизацией процесса создания мошеннических ресурсов, в том числе копирующих сайты известных брендов. Недавно мы подсчитали, что автоматизация процессов у кибермошенников достигла 80%, хотя еще четыре года назад не превышала 20%. То, что раньше занимало часы или даже недели, сейчас делается за несколько минут. Большая фишинговая кампания (с использованием бренда) может быть развернута в любой момент, атакуя лояльную аудиторию.

Станислав Гончаров, директор по развитию бизнеса Digital Risk Protection, F.A.C.C.T.

Из российских компаний Absolute Reports выделило активно работающую на международном рынке Group-IB. Еще в 2005–2006 гг. специалисты Group-IB проводили первые расследования распространения контрафактной продукции в интернете, создания фишинговых сайтов и других инцидентов, связанных с защитой

► спрогнозировать, как будет развиваться информационная атака;
► провести ситуационное моделирование – что произойдет при различных вариантах действий атакующих;
► провести сценарное моделирование – что произойдет при разных вариантах ваших действий;
► выбрать оптимальное решение;
► оценить риски.

Такова общая схема аналитической работы разведки. И подразделения, выполняющие подобную работу, все чаще появляются в российских компаниях.

В мире защитой бренда занимаются полторы тысячи аналитических центров. В их задачи входит защита бренда не только компаний, но и политиков, чиновников и даже государств. К сожалению, в России полноценных аналитических центров, выполняющих все перечисленное, нет. Если мы хотим участвовать в информационном противоборстве на равных, то должны уметь вести мониторинг, анализировать и огрызаться.

На российском рынке эта ниша отчасти занята компаниями, ранее предоставлявшими услуги политического пиара. Теперь к защите бренда подключились компании, специализирующиеся на кибербезопасности: сначала они занимались классической информационной безопасностью, потом стали внедрять технологию SIEM, которая обеспечивает анализ в реальном времени событий безопасности, происходящих в сетевых устройствах и приложениях. Потом сферу SIEM расширили, добавив анализ поведения сотрудников в защищенном контуре (DLP), потом – сбор и анализ событий за пределами контура в рамках Digital Risk Protection (DRP), в том числе атаки на бренд. Основные игроки этого сегмента – ИТ-компании, в которые инвестировал крупный бизнес: Сбер (BI.ZONE), «Ростелеком» («Ростелеком-Солар»).

Консорциум «Инфорус» помогает компаниям защищаться от информационных атак, и не только от атак на бренд, но и от дискредитации бизнеса и технологий. Наши клиенты – представители крупного бизнеса, которых постоянно атакуют. Например, «Рособоронэкспорт», торгующий оружием в 90 странах мира. Многие конкуренты спят и видят, как бы его из этих стран убрать. А «Норникель» атакуют по линии защиты экологии Севера. Если в Москве опрокинутую бочку с мазутом никто не заметит, то такая же бочка в Норильске будет подаваться как экологическая катастрофа с призывами гнать русских с этой планеты. Мы подобные атаки выявляем и предоставляем информацию клиентам для дальнейшей аналитической работы.

На российском рынке присутствует также ряд компаний, оценивающих здоровье бренда. Но только мониторинг – это ничего не дающее чтение вслух вчерашних газет. На оценке премиальности бренда далеко не уедешь, разве что заметишь, что уже проиграл. Нужна полноценная разведка, чтобы знать о противнике больше, чем он сам.

Андрей Бусаргин, руководитель департамента инновационной защиты бренда и интеллектуальной собственности, Group-IB

Digital Risk Protection снимает с компании бремя мониторинга интернета, изучения инструментов и больших массивов «сырых» данных. Но нужно не только выявлять проблемы, но и принимать меры: удалять фишинговые сайты, фейковые аккаунты топ-менеджеров. Для этого необходима юридическая подготовка, нужно знать, на что опираться, чтобы заблокировать ресурсы, как общаться с регуляторами, знать теорию по товарным знакам. В России таких специалистов мало.

бренда. Полученный опыт позволил создать технологии, на ранней стадии выявляющие мошеннические ресурсы и в автоматическом режиме собирающие доказательную базу. В 2008 г. появились первые клиенты, которым оказывалась услуга защиты бренда в интернете в круглосуточном режиме.

В 2017 г. Group-IB запустила централизованную систему, которая использует собственный движок поиска контрафактной продукции, технологии киберразведки (Threat Intelligence) и анализа больших данных. Система позволяет находить связи между сайтами, их владельцами и выявлять корреляцию между данными в соцсетях.

Несмотря на сильный репутационный удар – обвинение в разглашении гостайны и арест основателя и генерального директора компании Ильи Сачкова, – компания не прекратила работу. Чтобы не потерять зарубежных клиентов после событий февраля 2022 г., ей пришлось выделить в отдельную компанию часть, действующую в России. В апреле 2023 г. Group-IB сообщила, что продолжит работу на российском рынке под названием F.A.C.C.T. (Fight Against Cybercrime Technologies). Бренд Group-IB будет представлен только на международном рынке.

Российские решения

Для защиты бренда и цифровых активов на российском рынке компания F.A.C.C.T. предлагает платформу Digital Risk Protection. «Для автоматизированного выявления и классификации различных типов нарушений наше решение использует нейронные сети и многочисленные скоринги, что повышает скорость реагирования и его эффективность: 85% нарушений с незаконным использованием бренда устраняются в досудебном порядке. Согласно оценкам аналитиков F.A.C.C.T., решение обнаруживает пиратский контент в среднем за 30 мин и устраняет 80% нарушений в течение семи дней», – сообщил директор по развитию бизнеса Digital Risk Protection F.A.C.C.T. Станислав Гончаров.

Среди других российских игроков рынка DRP стоит обратить внимание на компании BI.ZONE, InfoSecurity (ГК Softline), «Лаборатория Касперского» и «Ростелеком-Солар».

Для мониторинга инфополя, утечек данных, выявления и нейтрализации угроз использования чужого бренда на фишинговых и мошеннических доменах компания BI.ZONE разработала решение BI.ZONE Brand Protection. Платформой класса DRP можно управлять самостоятельно или с экспертной поддержкой специалистов BI.ZONE. Платформа представлена в виде онлайн-кабинета, в котором работают сотрудники вендора и клиента. Возможна интеграция по API с системами клиента, что уменьшает время реакции на угрозы.

Защита осуществляется по трем направлениям:

- мониторинг открытых ресурсов (СМИ, соцсети);
- мониторинг мошеннических, фишинговых сайтов и доменов, распространяющих вредоносное ПО. Причем специалисты BI.ZONE не только выявляют такие домены, но и применяют меры досудебной блокировки;
- мониторинг даркнета, сведений об утечках, закрытых групп, телеграм-каналов, где мошенники обсуждают «серые» схемы.

«Лаборатория Касперского» проводит анализ комплексной безопасности компании в киберпространстве, в частности атак на бренд, в рамках продуктов и сервисов Kaspersky Threat Intelligence. Решения включают в себя платформу для управления данными о киберугрозах, поисковый портал о киберугрозах, сервисы отслеживания инфраструктур кибергруппировок, сервисы удаления фишинговых доменов, в том числе использующих цвета и товарные знаки защищаемой компании.

Специализированный сервис-провайдер InfoSecurity все направления DRP свел в единый продукт ETHIC – систему выявления и защиты от внешних цифровых угроз. В некоторых случаях компания передает заказчику «сырые» данные, но обычно решение предоставляется как сервис и заказчик выбирает его конфигурацию, исходя из специфичного для его отрасли или компании ландшафта угроз.

В 2023 г. часть команды разработчиков ETHIC перешла в компанию «Ростелеком-Солар», которая анонсировала запуск сервиса мониторинга внешних цифровых рисков – Solar AURA (Audit & Risk Assessment). Решение позволяет выявлять фишинг от имени компании (с последующей его блокировкой), утечки данных, признаки подготовки атак в даркнете. Solar AURA

предназначено для борьбы с незаконным использованием бренда, нелегальным применением эквайринга, махинациями с контрагентами.

Основные модули, которые подключаются отдельно или в комплексе DRP-решений:

- **«Антифишинг»** – обеспечивает полный цикл противодействия фишингу от лица компаний: от отслеживания опасных доменов с обнаружением фишинговых атак до их оперативной блокировки.
- **«Утечки»** – помогает оперативно выявлять факты компрометации чувствительной для заказчика информации в публичных источниках (персональные и учетные данные сотрудников, клиентов и партнеров; сведения об ИТ-инфраструктуре, включая репозитории с информацией, которая может быть использована в таргетированных атаках).
- **«Даркнет»** – отслеживает появление в даркнете угроз, нацеленных на заказчика (сообщения о готовящихся кибератаках и нелегальных услугах, предложения о «пробиве» или поиске точки входа в инфраструктуру компании, продаже баз данных и др.).
- **«Бренд компании»** – выявляет публичные ресурсы, включая аккаунты в соцсетях и мессенджерах, неправомерно использующие бренд компании-заказчика, а также отслеживает факты публикации мобильных приложений на неофициальных и небезопасных площадках.
- **«Личный бренд»** – отслеживает появление фейковых личных аккаунтов в соцсетях, случаи компрометации личных и корпоративных учетных данных, оценивает информационный фон вокруг персоналий компании, фиксирует появление негативных или компрометирующих публикаций.
- **«Медиаполе»** – выявляет наличие чувствительной для заказчика информации в открытом доступе: сведений об используемых средствах защиты информации, регламентах работы, особенностях ИТ-инфраструктуры и о лицах, ответственных за непрерывность производственных процессов.
- **«Безопасность финансов»** (предназначен в первую очередь для банков) – обнаруживает факты использования интернет-эквайринга банка для оплаты запрещенных в РФ услуг; собирает сведения о банковских картах, задействованных при отмывании или обналичивании денег, которые получены преступным путем; контролирует контент сайтов, использующих интернет-эквайринг защищаемого банка на предмет соответствия заявленному виду деятельности; предоставляет сведения для проверки контрагентов (выявляет компании и ИП, которые продаются или ранее продавались на «черном» рынке).

Агентства по борьбе с контрафактом

В отличие от компаний по кибербезопасности, фокусирующихся на технических аспектах, агентства больше внимания уделяют юридическим вопросам и специализируются на Brand Protection в западном понимании. Для предоставления услуг, как правило, используют имеющиеся на рынке инструменты, но иногда создают собственные. «Решения по защите бренда, такие как BrandMonitor, опираются на AI-алгоритмы, которые сканируют каждый сайт в интернете, соцсети и маркетплейсы в режиме 24/7 и автоматически блокируют сайты, с помощью которых конкуренты пытаются навредить вашему бренду. Более того, любые комментарии в социальных сетях подлежат тщательному анализу и при необходимости тоже блокируются», – сообщил руководитель юридического отдела BrandMonitor Даниил Шмырин.

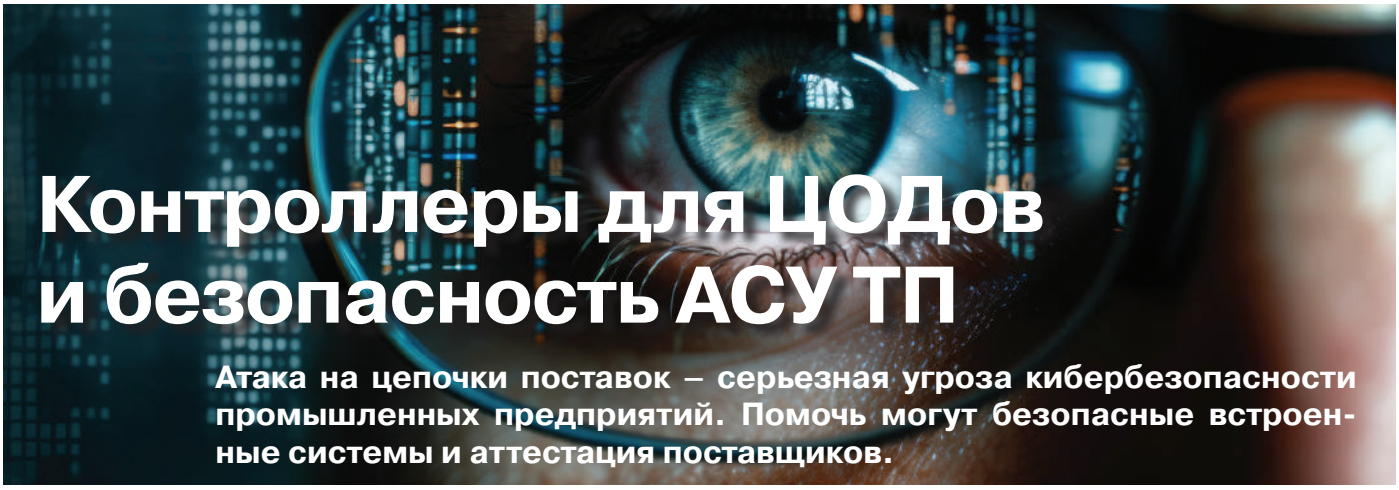
Среди других предлагающих комплексные услуги российских агентств стоит отметить BrandSecurity, разработавшую платформу BrandSecurity Rocket. Компания как в онлайне, так и в офлайне борется с контрафактом, «серым» импортом и пиратским контентом.

Снаряд и броня

«Число пользователей сегодня увеличивается скачкообразно – защитой бренда стали интересоваться те, кто раньше не обращал на нее внимания. Считалось, что DRP – это для крупного бизнеса», – констатировал эксперт центра мониторинга внешних цифровых угроз Solar AURA компании «Ростелеком-Солар» Александр Вураско. Сейчас сервисами стали интересоваться не только флагманы российского рынка, но и малые предприятия, средний чек услуги для которых – от миллиона рублей в год – выглядит экономически оправданным. За такие деньги даже одного квалифицированного специалиста по защите бренда в штат не возьмешь, а его еще надо найти и обеспечить необходимыми инструментами.

«Развитие DRP-направления – непрерывный процесс, так как появляются новые цифровые угрозы, которые необходимо выявлять и блокировать. Динамику рынка трудно точно спрогнозировать, но стоит отметить, что за последние два года интерес к этому направлению существенно вырос», – подтвердил тренд руководитель отдела анализа и оценки цифровых угроз InfoSecurity Константин Мельников.

Соревнование снаряда и брони – процесс бесконечный. Главное, что понимание важности защиты бренда в интернете у российского бизнеса растет. А это залог дальнейшего подъема рынка. ИКС



Контроллеры для ЦОДов и безопасность АСУ ТП

Атака на цепочки поставок – серьезная угроза кибербезопасности промышленных предприятий. Помочь могут безопасные встроенные системы и аттестация поставщиков.

Николай Носов

Новые технологии – новые риски

Еще 10 лет назад само понятие «информационная безопасность АСУ ТП» вызывало скептическую улыбку и мысли о нерациональном расходовании бюджетных средств. Какие могут быть проблемы у автоматизированных систем управления, использующих аналоговую технику? А если у них и имелся цифровой контур, то он был изолирован от интернета на физическом уровне. Не убеждала даже уничтожившая в 2010 г. около тысячи центрифуг на иранском ядерном объекте атака вируса Stuxnet – первого залпа войны нового типа. Первого вируса, разрушившего не только данные, но и оборудование в физическом мире.

Компьютеры несли неоспоримые преимущества, выгода превышала казавшийся маловероятным ущерб от использования новых технологий, и цифровизация все больше проникала в управление технологическими процессами. Росли риски, угрозы начали реализовываться, и скепсис по отношению к необходимости защиты АСУ ТП от киберугроз сошел на нет. Проблемы стали возникать даже на таких продвинутых в вопросах безопасности объектах, как АЭС.

Об одном из примеров – связанном с кибербезопасностью инциденте на американской АЭС им. Эдвина И. Хэтча – рассказала руководитель группы аналитиков по ИБ «Лаборатории Касперского» Екатерина Рудина. В рабочем контуре АЭС установили небольшую программу, которая собирала первичные данные о работе реактора и передавала их в основную систему, находящуюся в офисном контуре. Схема выглядела безопасной до одного из обновлений, когда новая версия стерла данные, а АСУ реактора восприняла их отсутствие как непонятную ситуацию и на всякий случай остановила реактор. По несчастливой случайности резервный блок в это время был остановлен для загрузки топлива. Запуск занял двое суток, ущерб компании от простоя составил $2 млн.

АСУ ТП стали интересовать хакеров. В 2013 г. бельгийская и голландская полиция сообщили об арестах по делу о переправке кокаина через порт Антверпена. Преступная группа использовала хакеров для доступа к компьютерным системам портовых компаний и терминалов, с помощью которых контролировала прием и разгрузку своих контейнеров с наркотиками. Не помогла и хорошая защита внешнего контура – преступники пронесли в офисы компаний специальную аппаратуру для перехвата и передачи информации, вмонтированную в обычные электрические удлинители.

Атаки на цепочки поставок

Проблемы безопасности промышленных предприятий резко обострились после февраля 2022 г. К хакерам добавились политически мотивированные преступники, термин «кибервойна» стал употребляться регулярно, заговорили о спонсируемых государствами хакерских группировках. «В целом наши субъекты КИИ так или иначе справились с проблемой – благодаря тому, что “спрятались в домик”. По максимуму отключили внешние интерфейсы, закрутили гайки, отмобилизовали персонал. В публичное пространство не ушла информация о крупных взломах», – констатировал директор компании iGrids («Интеллектуальные сети») Максим Никандров.

Во многом это заслуга регуляторов. Были выпущены требования к субъектам КИИ – приказы ФСТЭК, ФСБ и другие документы, связанные с выполнением закона № ФЗ-187 «О безопасности критической информационной инфраструктуры РФ». И субъекты КИИ вынуждены заниматься безопасностью. Этот путь уже проверен на банках. ЦБ РФ был одним из первых регуляторов, который заставил подопечных принять меры по защите своих компьютерных систем, и теперь банки – одни из наиболее защищенных объектов КИИ.

Однако не так все безоблачно. Не сумев справиться с крупными игроками, преступники обратили внимание на небольшие компании, разработчиков, субподрядчиков. Атаки и взломы продолжаются. Например, в мае накануне партнерской конференции «Инфотекса» хакеры опубликовали базу данных зарегистрированных пользователей сайта компании, в июне в сеть утекли данные клиентов магазинов «Ашан» и «Твой дом». В большинстве случаев атаки проводились через уязвимости у поставщиков программного обеспечения или услуг.

Субъекты КИИ используют в том числе продукцию мелких компаний, которые в силу отсутствия денег или компетенций зачастую не обращают внимание на информационную безопасность. Требования к этим компаниям не предъявляются, а затраты на безопасность чувствительны для бюджета.

Ситуацию усугубляет уход с российского рынка ведущих вендоров средств информационной безопасности, предлагавших лучшие по соотношению «цена – качество» продукты. Выросшие цены ударили прежде всего по небольшим компаниям, решившим укрепить свою безопасность. Неважно обстоит дело и с защитой персональных данных, утечка которых упрощает фишинговые и другие персонализированные атаки на сотрудников организаций. Если же законодательно транслировать требования к субъектам КИИ на подрядчиков, то небольшие компании не смогут их выполнить и уйдут с рынка, а оставшиеся крупные игроки резко поднимут цены. Это ударит и по субъектам КИИ.

Встраиваемые операционные системы и ЦОДы

Защита от атак на цепочку поставок заботит все компании и предприятия. Но защита АСУ ТП имеет особенности, связанные прежде всего с массовым использованием микропроцессорных программируемых логических контроллеров (ПЛК) и интеллектуальных электронных устройств (ИЭУ). Доцент кафедры релейной защиты и автоматизации энергосистем НИУ МЭИ Владимир Карантаев подчеркнул важность обеспечения безопасности встраиваемых в ПЛК и ИЭУ операционных систем, которые предъявляют специфические требования к характеристикам и доступным ресурсам.

В качестве примера он привел релейную защиту от коротких замыканий на подстанциях, главные требования к которой – селективность, чувствительность, быстродействие и надежность. Раньше использовались электромеханические устройства – их работа зависела только от конструктива и уставок срабатывания, задававшихся механическим путем. Теперь используются ИЭУ, которые являются программно-аппаратными комплексами, что делает устройство потенциально уязвимым для хакеров. Причем, как показали исследования, наложенных средств безопасности (антивирусов, межсетевых экранов) для эффективной защиты недостаточно. Безопасность обеспечивают только решения, встроенные в операционную систему. И ОС должна быть не общего назначения, а специализированная, удовлетворяющая политикам информационной безопасности, с маленьким ядром, которое сокращает поверхность атаки и ограничивает функционал лишь необходимыми для работы командами.

Атаки на электрические подстанции можно рассматривать как атаки на цепочку поставок, в данном случае поставок электричества, необходимого для работы заводов, предприятий и учреждений. Тем более что далеко не все из них, подобно дата-центрам, готовы к такой ситуации и смогут перейти на работу с ИБП и дизель-генераторами.

Да и ЦОДам, в инженерных системах которых широко используются ПЛК и ИЭУ, стоит учесть возможность атак на встраиваемые операционные системы. По крайней мере предусмотреть такую возможность в модели угроз и обратить внимание разработчиков инженерных систем на соответствующие риски.

Главная проблема создания российских технологически независимых встроенных решений, как указал В. Карантаев, – неопределенность с микропроцессорами. До начала СВО были доступны процессоры как минимум двух архитектур – «Эльбрус» и «Байкал». Сейчас поставки этих процессоров заблокированы из-за того, что заводы на Тайване присоединились к санкциям. Перспективной выглядит архитектура RISC-V, но и здесь возникают вопросы с производством.

Вторая проблема – недостаток внимания к созданию российских защищенных встраиваемых ОС, которые являются основой АСУ ТП, да и всей промышленной автоматизации в целом. Используемые в настоящее время встроенные ОС, в том числе массово применяемые системы из недружественных стран, не соответствуют научно обоснованным требованиям по защите. Чтобы обеспечить безопасное функционирование нашей промышленности, нужна поддержка работ данной тематики со стороны государства.

Телекоммуникационные шкафы

Компания Art Engineering представляет линейку 19-дюймовых телекоммуникационных шкафов, предназначенных для размещения сетевого и вспомогательного оборудования.

В линейку входят шкафы высотой от 42U до 48U с возможностью монтажа дополнительных аксессуаров, в том числе органайзеров для размещения кабелей, магнитных заглушек, кронштейнов для крепления PDU и усиленных низкопрофильных роликов. Шкафы имеют легкосъемные боковые панели на защелках, а также две пары 19-дюймовых направляющих из стали толщиной 2 мм, которые регулируются по глубине установки. Рама и двери изготовлены из высококачественной конструкционной стали толщиной 2 мм, крыша и панели – 1,5 мм.

Основные характеристики шкафов:
- ширина – 600, 750 или 800 мм;
- глубина – 1070, 1200 мм;
- нагрузочная способность – 1600 кг;
- доля перфорации в передней и задней дверцах превышает 75%.

Шкафы поставляются в разобранном виде в плоской картонной упаковке, что позволяет сократить расходы на логистику. Гарантийный срок на продукцию – шесть лет.

art-engineer.ru

Модульные ИБП для критических нагрузок

Компания «Систэм Электрик» вывела на рынок модульные ИБП серии Excelente. Они обеспечивают защиту критически важных нагрузок и служат заменой широко известной серии ИБП Symmetra от APC. ИБП построены по модульному принципу, что позволяет проводить «горячую» замену силовых модулей, модулей управления и байпаса.

ИБП серии Excelente обладают единичным коэффициентом мощности по выходу (PF = 1) на всем диапазоне рабочих температур, что дает возможность рассчитывать необходимый уровень защиты для существующей инфраструктуры. До шести ИБП можно подключить в параллель для наращивания выходной мощности до 3,6 МВт.

В серию входят три продукта: Excelente VM (50–300 кВА), Excelente VL (350–600 кВА) и Excelente VX (100–600 кВА).

ИБП серии имеют компактные силовые модули высотой 3U (50 кВт для VM/VL и 100 кВт для VX), дублированные платы управления и усиленное зарядное устройство, обеспечивающее быстрый заряд как свинцовых, так и литиевых батарей.

Основные характеристики:
- диапазон входного напряжения – 138–485 В;
- диапазон входной частоты – 40–70 Гц;
- коэффициент искажения THDi ≤ 3%;
- коэффициент искажения THDu ≤ 1%;
- выходной коэффициент мощности 1;
- подключение от 30 до 50 батарей в одной цепи;
- КПД в режиме двойного преобразования 96,6%;
- ширина конструктива – 600 мм (VM), 1200 мм (VL) и 800 мм (VX).

Гарантийный срок на трехфазные ИБП Systeme Electric составляет два года.

systeme.ru

Накопитель электроэнергии на базе LFP

Компания ENERGON представила DELTA UDL-R – литий-железо-фосфатный ($LiFePO_4$) накопитель электроэнергии, изготавливаемый полностью на территории РФ.

Он рассчитан на время автономной работы от 30 мин, совместим с любыми трехфазными ИБП и может выступать в качестве замены любых свинцовых аккумуляторов. UDL-R оснащен системой управления батарейным массивом (BMS) также российской разработки.

Накопители могут использоваться на объектах первой категории надежности электроснабжения (в медицинских учреждениях для резервирования электропитания томографов, систем жизнеобеспечения, реанимационного оборудования, в государственных и муниципальных структурах, на коммерческих объектах с большим числом потребителей электроэнергии). UDL-R могут устанавливаться и на солнечных электростанциях.

Накопители DELTA UDL-R поддерживают постоянный ток напряжением до 512 В. Энергоемкость шкафа на 512 В составляет до 50 кВт·ч, и этот объем UDL-R отдает за 30 мин. Максимальная постоянная разрядная мощность – 100 кВт. Для построения энергоемких решений (до 400 кВт) можно объединять до восьми UDL-R в параллель. Устройство выдерживает 3 тыс. циклов заряда-разряда при глубине разряда 100%, что равноценно 15-летней службе.

В UDL-R имеется встроенный автоматический выключатель постоянного тока, который защищает силовую часть от короткого замыкания. Защита от перегрева и глубокого разряда обеспечивается средствами BMS. Для мониторинга работы таких массивов применяется встроенный инструмент с веб-интерфейсом, работающий через Wi-Fi-соединение. С помощью специального бесплатного ПО также беспроводным способом можно провести полноценную диагностику.

energon.ru

Бизнес-партнер

Модульные ИБП для ЦОДов

В I квартале 2023 г. компания ДКС вывела на рынок линейку мощных модульных ИБП серии TRIO MD, дополнившую существующий ассортимент моноблочных ИБП TRIO.

TRIO MD – это вертикально и горизонтально масштабируемое решение для защиты критической нагрузки с высокой плотностью размещения, ориентированное в первую очередь на центры обработки данных и ИТ-объекты. При необходимости решение масштабируется от 25 до 600 кВт в одной системной стойке и до 2,4 МВт – в параллельной системе из четырех системных стоек.

Доступность модульного ИБП из новой линейки с резервированием 3 + 1 оценивается в 0,999999 (шесть девяток) вместо 0,99999 (пять девяток) для моноблочного ИБП с резервированием 1 + 1, а среднее время восстановления (MTTR) при тех же схемах резервирования – всего лишь в 0,5 ч вместо 6 ч для моноблочных ИБП.

Достоинства линейки TRIO MD:

▶ Простота запуска, эксплуатации и обслуживания системы. Для проведения работ не требуется какого-либо специализированного ПО с ограниченным доступом. Все необходимые настройки осуществляются с удобного русифицированного дисплея.

▶ Соответствие ИБП характеристикам, заявленным в документации. Характеристики были подтверждены в ходе испытаний, проведенных независимой лабораторией.

▶ Возможность «горячей» замены любых компонентов. Конструктив новых ИБП предусматривает возможность «горячей» замены силовых модулей, модуля байпаса и модуля управления. Замена с легкостью может быть осуществлена персоналом компании-заказчика. Последовательность действий по замене подробно изложена в инструкции по эксплуатации, подготовленной ДКС.

▶ Все возможные опции представлены в базовом комплекте поставки. Заказчикам модульных ИБП не нужно приобретать дополнительные компоненты для доступа к дополнительным опциям. ИБП поставляются в полной комплектации.

▶ Наличие ИБП на складе компании ДКС в Твери. Заказанный ИБП можно получить в срок от одной недели.

DKC
dkc.ru

РЕКЛАМА В НОМЕРЕ

Указатель фирм и организаций

Учредитель журнала «ИнформКурьер-Связь»:

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

Eurasia Data Center & Cloud Forum

3-я международная конференция и выставка

Узбекистан, Ташкент

3–4 октября 2023

International Hotel Tashkent

Data Center & Cloud Kazakhstan

6-я международная конференция и выставка

Казахстан, Алматы

23–26 октября 2023

The Rixos Hotel Almaty

Основная задача форумов – обмен знаниями и наилучшим опытом в области проектирования, построения и эксплуатации ЦОДов, а также предоставления услуг на их базе.

- Перспективы развития рынка дата-центров и облачного провайдинга
- Экономические модели и бизнес ЦОДов
- Инженерная инфраструктура ЦОДов
- ИТ-решения и облачные сервисы

DCFORUM.UZ

ПОДРОБНО О ПРОГРАММЕ И УЧАСТНИКАХ НА САЙТАХ КОНФЕРЕНЦИЙ

DCFORUM.KZ

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

Организаторы: ИКС Медиа, iKS Consulting

При поддержке и участии: Координационный совет по ЦОДам и облачным технологиям, Автономная некоммерческая организация; uptime INSTITUTE

KEY POINT GROUP

РЕГИОНАЛЬНАЯ СЕТЬ ЦОД

ВАЖЕН КАЖДЫЙ!

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

keypoint-group.ru