ТЕМА НОМЕРА

НАДЕЖНОСТЬ СИСТЕМ ИБП. ЧТО ВЫБИРАЮТ ЦОДЫ

ИнформКурьер-Связь
ИКС
издается с 1992 года

Роман Шмаков

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

Наша стратегия – развитие комплексной экосистемы

CLIVET

Inspiring Solutions since 1989

Решения
для центров обработки данных

НАШИ ПРЕИМУЩЕСТВА:

- ✔ Широкий выбор опционального оснащения оборудования:
  - TURBO — быстрый перезапуск **(Fast Restart)**
  - UPS — встроенный источник бесперебойного питания **(UPS)**
  - устройство автоматического ввода резерва **(ATyS G)**
  - −40 — система подогрева шкафов автоматики для работы при низких t (подогрев шкафов автоматики, исполнение вентиляторов **до -40 °C**)
- ✔ Испытания и приёмка оборудования на заводах производителя в присутствии заказчика
- ✔ Надёжная логистика и складская программа
- ✔ Техническое сопровождение и оперативный сервис

Центробежные компрессоры Back-to-Back дизайна
WDHT-CN
880-4600 кВт

Безмасляные центробежные компрессоры Magnetic
WTHT-CNA
600-4400 кВт

Инверторные винтовые компрессоры
WDAT-CN HV FCD
350-1300 кВт

Винтовые компрессоры
WDAT-SL3 FC
460-1400 кВт

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: 16.08.24.
Дата выхода в свет: 27.08.24.
Тираж 5 000 экз. Свободная цена.
Формат 64x84/8
Типография: ООО "ПРОПЕЧАТЬ",
адрес типографии 119618, г. Москва,
Боровское ш., дом 2А, корп. 4, кв. 260.

ISSN 0869-7973

12+

Выставка достижений цодостроения

Год назад на московском форуме «ЦОД» свои продукты и сервисы представили более 60 компаний. Честно говоря, я думал, что это предел. Ошибся: в этом году таких компаний свыше 80...

Что привлекает на российский рынок ЦОДов все больше и больше участников? Этот вопрос за последний год я задавал многим новым игрокам. Отвечают все примерно одинаково: «отличные перспективы». Рынок стабильно растет, и темпы роста двухзначные. Цифровизация всех сфер экономики, госуправления, общественной и личной жизни набирает обороты. А тут еще дополнительный катализатор в виде искусственного интеллекта.

Говоря о цодостроителях, отмечу активизацию большой группы новых игроков – девелоперов. Практически все основные застройщики, по крайней мере в Москве, продемонстрировали интерес к рынку ЦОДов. Одни, например Alcon Group, PNK Group, «МонАрх», ФСК, активно строят или даже сдали свои первые объекты в эксплуатацию. Другие – большинство – присматриваются. Можно долго спорить о бизнес-моделях, используемых девелоперами, из которых наиболее популярная – «построить и продать (сдать в долгосрочную аренду)», но то, что они уже внесли существенный вклад в увеличение числа стойко-мест, очевидно.

Если говорить о поставщиках продуктов для ЦОДов, то их привлекают не только высокие темпы роста рынка, но и несформировавшиеся пока вендорлисты ключевых игроков. Прогнозировалось, что за год-два опустевшие (после ухода в 2022 г. западных производителей) сегменты рынка оборудования будут быстро заполнены. Не сложилось. Предложений много, но проверку выдерживают далеко не все. Простая перепродажа китайских продуктов под видом отечественных не обрела большого числа поклонников среди серьезных заказчиков. Нужны сервис, экспертиза и приверженность локализации ради снижения рисков. Рынок все еще остается турбулентным, кто-то уходит, кто-то приходит – много новых игроков и новых предложений.

На форуме «ЦОД» нас ждет «ралли вендоров» – соревнование поставщиков за внимание заказчиков, которые смогут детально ознакомиться с решениями большинства игроков на рынке, а значит, сделать максимально информированный и обоснованный выбор. Победители в «ралли» получат наибольшее число заказов и соответственно значимую долю соответствующего рынка.

До встречи на «ЦОД-2024»,
Александр Барсков

Надежность систем ИБП → с.28

с. 4

Российские ЦОДы: в тренде – комплексность

с. 22

ЦОД-прогнозы 2024. Окончание

с. 46

Г. Дрягин. Среда общих данных как основа BIM/TIM

с. 69

О. Федоров. Пять принципов бесперебойной работы ИТ-инфраструктуры

Н. Носов. Не по правилам

с. 72

Российские ЦОДы: в тренде – комплексность

В условиях непрерывно меняющегося рынка дата-центрам нужны вендоры-интеграторы, обеспечивающие комплексную сервисную поддержку и отвечающие своим брендом за надежность выбранных инженерных решений.

Рост рынка

Ежегодно проводимая «ИКС-Медиа» конференция Data Center Design & Engineering давно стала главной площадкой для обсуждения достижений и проблем развития рынка инженерных систем для ЦОДов в России. Неудивительно, что и состоявшаяся в мае 2024 г. 11-я по счету конференция вызвала большой интерес – ее посетили более 800 делегатов со всей страны.

Перспективы рынка ЦОДов вполне оптимистичны. Согласно данным iKS-Consulting, число стойко-мест в коммерческих ЦОДах вырастет с 70,1 тыс. в 2023 г. до 115,3 тыс. в 2027 г., так что производители инженерных систем для дата-центров без заказов точно не останутся.

Вопрос только в том, кого выберут заказчики, кто лучше ответит на потребности рынка, какой стратегии придерживаться работающим на российском рынке компаниям. Темы актуальные, что подтвердили переполненные залы и активные обсуждения в выставочной зоне конференции.

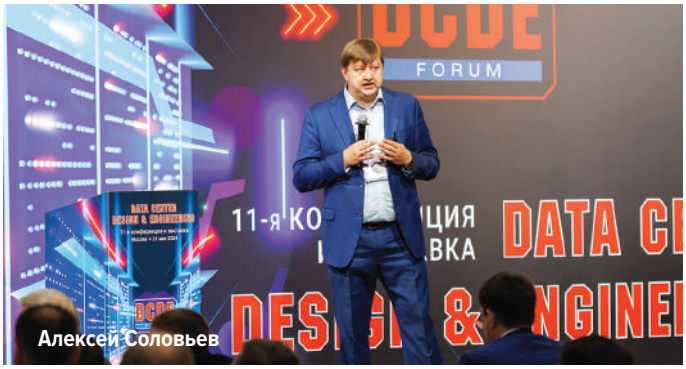
Запрос на комплексную сервисную поддержку

Российские вендоры инженерных систем успешно справились с проблемами, возникшими после ухода с рынка зарубежных производителей, переняли и развили лучшие практики мировых лидеров. Как отметил технический директор управления «ИТ-решения» компании Systeme Electric Алексей Соловьев, компетенции даже расширились, так как российским инженерам, уже имевшим опыт наладки и сопровождения продукции мирового вендора, пришлось поддерживать оборудование и других ушедших компаний, что обогатило их экспертизу и позволило разрабатывать более совершенные продукты.

Кроме того, отечественные вендоры стали тщательнее изучать потребности клиентов. Если раньше основными заказчиками аналитического агентства iKS-Consulting были иностранные вендоры, то только в текущем году проведены уже три исследования рынка в сотрудничестве с российскими игроками. Совместно с «Парус электро» выпущена аналитическая записка «Надежность систем ИБП», с C3 Solution – «Сервис для ИБП», с Systeme Electric – «Инженерная инфраструктура ЦОДов. Комплексный подход». Последнее исследование дало несколько неожиданный результат: сокращение расходов на эксплуатацию за счет предоставления всех продуктов из одних рук – вроде бы, очевидное преимущество – оказалось не столь важным для заказчиков. Главными были названы ответственность за решение в целом и комплексная сервисная поддержка.

Правда, одно другому не мешает. На аналитической сессии представители дата-центров, сравнивая моновендорные ЦОДы, для которых основные узлы инфраструктуры – системы электропитания, охлаждения и размещения ИТ-оборудования (стойки/шкафы) – поставляются одним вендором, и проекты на основе решений разных производителей, отметили, что различие непринципиально. Нужно выбирать лучшее из представленного на рынке с учетом возможностей поставщика поддерживать свои продукты.


Алексей Волков



Алексей Соловьев

Сегодня, когда мировые лидеры ушли с российского рынка, а оценить качество, надежность и совместимость решений новых компаний с еще не устоявшейся репутацией сложно даже крупным заказчикам, увеличивается спрос на вендоров-интеграторов, отвечающих своим брендом за решение в целом или хотя бы за основные узлы инженерной инфраструктуры ЦОДа. Обеспечить комплексную сервисную поддержку и взять ответственность за все решение проще, если вендор поставляет собственное оборудование, которое хорошо знает и интеграцией которого занимался еще на этапе разработки.

Все из одних рук

«Скромность украшает мужчину, но зачем настоящему мужчине украшения?», – говорил чешский писатель Ярослав Гашек. C3 Solutions украшения точно ни к чему – в продемонстрированном на конференции видеоролике команда компании позиционировалась как сборная лучших профессионалов своего дела, сравнимая со сборной СССР по хоккею.

Впрочем, компании действительно есть чем гордиться. Если раньше C3 Solutions ассоциировалась в основном с запоминающейся рекламой и качественными российскими стойками (шкафами), а амбиции стать российской Schneider Electric, предоставляющей всю палитру инженерных решений для ЦОДов, вызывали улыбку, то сейчас все серьезно. С появлением в портфеле компании прецизионных кондиционеров на ее решениях можно построить моновендорный ЦОД. Как отметил руководитель направления систем резервирования и электропитания C3 Solutions Алексей Волков, компания поставляет под ключ всю ИТ-инженерию, включая системы мониторинга, кондиционирования, бесперебойного питания, СКС, системы изоляции и монтажные шкафы. И все это с технической поддержкой и кастомизацией под крупных заказчиков. Моновендорные ЦОДы на решениях C3 Solutions уже появились, хотя и небольшие. Так, в Белгороде под патронажем Сбербанка развернут микроЦОД в кампусе проекта ИТ-образования «Школа 21».

Среди представленных компанией на выставке новинок – PDU на процессорах «Байкал», это продукт с полным, вплоть до микроэлектроники, импортозамещением. Непонятен только размер партии, на которую хватит запасов теперь такого дефицитного российского процессора.

На плечах гиганта

Российской компании Systeme Electric, на продукции которой тоже можно строить моновендорный ЦОД, было проще – в наследство от именитой французской предшественницы она получила производственные мощности, налаженные технологические процессы и сотрудников с квалификацией мирового уровня, в том числе в области комплексного сопровождения ЦОДов. Такое сопровождение всех этапов жизненного цикла дата-центра, от планирования до эксплуатации и модернизации, становится, как отметил А. Соловьев, особенно актуальным в условиях дефицита кадров.

С дефицитом же кадров помогает справиться повышающая производительность труда автоматизация. На конференции были представлены ПО для мониторинга DC Guard и поддерживающая техническое обслуживание инженерной инфраструктуры система Systeme Maintenance, включающая оперативно-диагностический модуль, паспортизацию оборудования на базе дерева активов и модуль обработки и анализа информации. Осмотр, диагностику, наладку и ремонт оборудования можно будет выполнять силами даже неквалифицированного специалиста, если в его экипировку входят очки дополненной реальности. Через эти очки ему будет дистанционно помогать высококвалифицированный специалист, использующий модуль «Удаленный эксперт».

От кабель-каналов до СКС

Как производителя и поставщика комплексных инженерных решений для ЦОДов позиционирует себя и ДКС. Компания, четверть века назад начавшая бизнес с производства гофрированных труб для электропроводки, освоила производство практически всего, что необходимо для развертывания инженерной инфраструктуры ЦОДа. В числе выделенных директором департамента цифровой энергетики Денисом Власовым решений – PDU, оптические и проволочные лотки, кабельные каналы, модульные ИБП. С 2022 г. компания предлагает рынку высокоплотную оптическую подсистему для ЦОДов, в которую входят многопрофильная коммутационная панель, претерминированные кассеты и сборки. Для построения моновендорного ЦОДа не хватает систем охлаждения, но и без этого номенклатура инженерных решений выглядит внушительно.

Большое внимание уделяется сервисной поддержке. Библиотека готовых чертежей продуктов и динамиче-

ские блоки облегчают проектирование, разработанные плагины позволяют проектировать инженерные коммуникации в формате 3D, базы данных для nanoCAD содержат элементы кабеленесущих систем и разветвительные коробки. А главное – есть давно сформировавшийся российский бренд, вызывающий доверие у заказчиков.

Комплексность ИБП

Даже производители ИБП стали позиционировать себя как поставщики комплексных решений. Михаил Вазисов, генеральный менеджер компании Ippon, просто заряжал слушателей энергией, с которой рассказывал о комплексных решениях на базе продукции своей компании. Задолго до ухода с рынка западных вендоров Ippon воспринималась как производитель качественных однофазных решений, а теперь она успешно вступила в борьбу за освободившийся рынок «тяжелых», трехфазных ИБП.

Из представленных на выставке новинок можно отметить напольные модульные ИБП BlackRock мощностью до 600 кВА. Функция «горячей» замены модулей позволяет проводить регламентные и ремонтные работы без отключения нагрузки от электропитания.

Компания не претендует на комплексные поставки всего инженерного оборудования, сконцентрировавшись на ИБП. Но в этом направлении развивается активно, предлагая не только ИБП, но и аккумуляторные батареи и щиты электропитания. Особое внимание Ippon уделяет обучению и сервисной поддержке партнеров, используя для этого открытый в подмосковном Красногорске технический центр.

Друзья с Востока

Осознали новую реальность российского рынка и китайские компании. Практически ушел, опасаясь вторичных санкций, лидер – Huawei, зато активизировались игроки, не столь зависящие от западных рынков. Например, на наш рынок выходит такая крупная компания, как Haiwu, которая для работы в России решила использовать бренд Cybersys. Как сообщил ее вице-президент Джефф Чжан, по данным исследовательской компании Omdia, Haiwu в 2023 г. заняла пятое место в мировом рейтинге производителей систем охлаждения для ЦОДов.

Haiwu поставляет практически все основное инженерное оборудование для ЦОДов, включая системы бесперебойного питания, шкафы, решения для холодных и горячих коридоров, а также модульные, контейнерные ЦОДы и микроЦОДы.

Попрактиковаться в английском с симпатичной китайской девушкой на стенде Cybersys было приятно, но все же без русскоязычного представительства на российском рынке зарубежной компании будет трудно. Это хорошо поняла и китайская компания TICA, работающая в России через своего дистрибьютора – Data Center Group.

TICA – один из крупнейших китайских производителей систем охлаждения для ЦОДов. Она предлагает широкий спектр решений: приточно-вытяжные установки, прецизионные кондиционеры мощностью до 300 кВт, холодные стены мощностью до 600 кВт, драйкулеры мощностью до 1400 кВт и чиллеры мощностью до 13 000 кВт.

Отвечая на вопрос нашего издания, коммерческий директор Data Center Group Тимур Шабаев пояснил, что компания не имела и не имеет широко обсуждаемых в СМИ проблем с платежами в китайских банках, поскольку является их постоянным клиентом. И заверил, что TICA не пойдет по пути Huawei, так как дорожит российским рынком, не имеет значительного присутствия на рынках недружественных стран.

Вода и огонь

Даже мировые лидеры рынка инженерных систем для ЦОДов не могут закрыть продукцией под своим брендом все требуемые дата-центрам позиции. Это тем более верно, когда речь идет о сильно зависящих от локального регулирования системах пожаротушения. Изменения на рынке, вызванные событиями последних лет, наложили

Михаил Вазисов

Джефф Чжан

Тимур Шабаев

Михаил Кочетков

Александр Мартынюк

Артем Стенюшкин

отпечаток и на эту довольно консервативную отрасль. Так, генеральный директор Холдинга ОСК групп Михаил Кочетков отметил сложности с поставками газа для пожаротушения даже из Китая – они как раз связаны с задержками прохождения платежей в китайских банках.

В этих условиях дополнительные преимущества получают системы пожаротушения мелкораспыленной водой (водяным туманом), такие как представленная на конференции система ИНТРА-ФОГ. М. Кочетков развеял ложные представления о высокой опасности тушения водяным туманом компьютерной электроники, а в видеоролике с тестовым пожаротушением продемонстрировал, как за пару минут система гасит пожар в стойке.

Вопросы проектирования

Вендоры инженерных систем поставляют библиотеки чертежей своих устройств для компьютерного проектирования и моделирования ЦОДов, но непосредственно проектированием должны заниматься профессионалы. Проектировщики, как отметил исполнительный директор «Ди Си Квадрат» Александр Мартынюк, могут реализовать самые смелые запросы заказчиков, например, дата-центры с высоконагруженными стойками. Хотя в коммерческих, ориентированных на широкий круг заказчиков ЦОДах востребованность таких стоек пока невысока, в корпоративных, где важнее не экономическая эффективность, а решение поставленной задачи, уже и российские заказчики иногда запрашивают стойки с нагрузкой более 50 кВт. А на мировом рынке, согласно данным Uptime Institute, доля таких стоек в 2022 г. составила 5%.

При этом проектирование тоже должно быть комплексным, учитывать время и место работ, особенности используемых инженерных решений. По словам BIM-менеджера компании «Свободные Технологии Инжиниринг» Геннадия Дрягина, нужна среда общих данных (СОД) – комплекс программно-технических средств, представляющих единый источник данных, обеспечивающий совместное использование информации всеми участниками инвестиционно-строительного проекта.

Основная задача СОД – централизация проектной информации для совместного доступа, отслеживания ее статуса и версионности. Отдельно выделяются СОД, позволяющие взаимодействовать с BIM-данными. Под взаимодействием понимается не только хранение, но и просмотр и анализ компонентов. Загрузка BIM-данных в СОД возможна как через форматы разработки информационных моделей, так и через промежуточные форматы. Внедрение таких систем, как подчеркнул Г. Дрягин, не так трудоемко, как изменение систем разработки документации или информационных моделей.

Высокое искусство

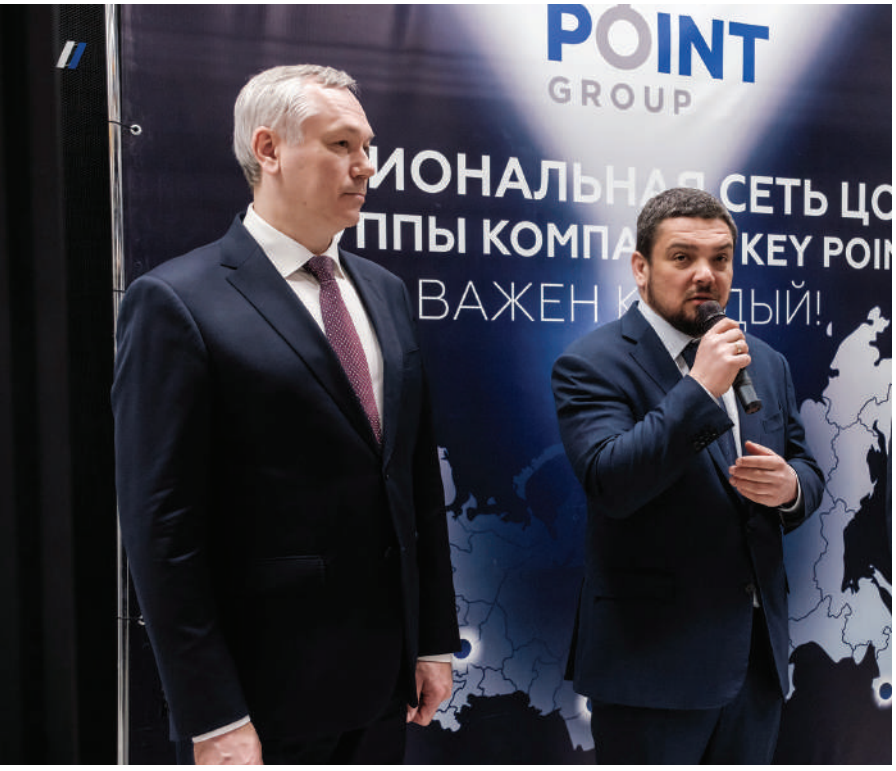
Проекты ЦОДов всегда были индивидуальными, а сегодня, когда доступность компонентов инженерных систем не определена априори, они приближаются к произведению искусства. И уж тем более к искусству можно отнести внешний дизайн, то, что непосредственно видит заказчик. Поговорка «встречают по одежке» справедлива и для дата-центров. Эстетическую важность решений подчеркивает слово «ART» в названии компании ART Engineering, коммерческий директор которой Артем Стенюшкин рассказал о предлагаемой рынку системе изоляции коридоров Monument. Так, комплектация Premium позволяет добиваться индивидуальной проработки в системе любой детали, наносить на поверхность требуемые заказчику логотипы и изображения, размещать в коридоре стоечные шкафы разной высоты.

Несмотря на существующие трудности, отрасль инженерных решений для ЦОДов уверенно развивается. Спрос на продукцию есть и будет только расти, к санкциям российские компании адаптировались. Возвращение мировых лидеров (если такое случится) станет, конечно, положительным фактором, усиливающим конкуренцию и, как следствие, повышающим уровень цинженерных решений. Но прежнюю долю рынка зарубежные вендоры уже занять не смогут. Российские производители окрепли, доверие к ним выросло, и клиентов они без боя не отдадут.

Николай Носов

Самый большой в Сибири

26 апреля 2024 г. в Промышленно-логистическом парке Новосибирской области состоялась торжественная церемония открытия I очереди ЦОДа группы компаний Key Point. Новый дата-центр стал самым большим коммерческим ЦОДом в Сибирском регионе и одним из самых крупных за пределами Москвы и Санкт-Петербурга.



Губернатор Новосибирской области Андрей Травников

«Новосибирская область становится безоговорочным лидером по развитию цифровой инфраструктуры, настоящим ИТ-центром нашей страны за Уралом... Мы видим, что инвесторы понимают перспективу и закладывают возможность для наращивания мощностей, в том числе по проекту Key Point. Будем оказывать содействие, потому что этот проект для нас знаковый, важный, интересный, заслуживающий всяческого внимания».

Емкость I очереди ЦОДа составляет 440 ИТ-стоек. Общая проектная емкость центра – 880 ИТ-стоек по 7 кВт каждая. Новый дата-центр соответствует всем международным стандартам обеспечения стабильной работы вычислительных систем любого поколения и успешно прошел двухступенчатую процедуру сертификации Uptime Institute по уровню надежности Tier III.

ЦОД построен с максимальным использованием российского оборудования. Генеральным проектировщиком и подрядчиком объекта выступила компания «Свободные Технологии Инжиниринг», опыт и профессионализм специалистов которой позволили реализовать проект на высоком технологическом уровне.

Для охлаждения серверных залов используются «холодные стены» (системы класса LSV), а для повышения эффективности охлаждения – системы изоляции горячих коридоров

Внутри энергомодуля с ИБП и АКБ

Внешние энергомодули с трансформаторными подстанциями и ДГУ

Основатель ГК Key Point Евгений Вирцер

«ЦОД был построен всего за 11 месяцев, что стало возможным благодаря слаженной работе команды опытных инженеров и использованию префаб-решений – отдельных узлов, которые изготавливаются в заводских условиях и сокращают количество операций на строительной площадке».

Строительство объекта было завершено в рекордно сжатые сроки. Первый камень новосибирского ЦОДа был заложен 11 апреля 2023 г., а уже в феврале текущего года I очередь дата-центра успешно прошла сертификацию Uptime Institute, эксперты которого высоко оценили инженерные решения, примененные в ЦОДе. По результатам испытаний дата-центру присвоен уровень Tier III Constructed Facility. Построить объект за такой короткий срок стало возможным в том числе благодаря использованию префаб-решений производства ART Engineering.

Обслуживать ЦОД будут 45 высококвалифицированных специалистов, причем все они – местные жители. Благодаря реализации проекта регион получил не только передовую инфраструктуру, но и новые рабочие места. Услугами ЦОДа уже начали пользоваться как региональные компании разных отраслей, так и крупнейшие телекоммуникационные операторы страны, активно развивающие свои ИТ-сервисы в Новосибирской области.

Чиллеры с функцией фрикулинга обеспечивают охлаждение водно-гликолевой смеси для подачи на «холодную стену»

ЦОДы прирастают Сибирью

По прогнозу iKS-Consulting, в ближайшие три года емкость коммерческих ЦОДов в Новосибирске удвоится, и столица Сибири сможет претендовать на то, чтобы стать третьей крупной агломерацией ЦОДов – после Москвы и Санкт-Петербурга.

«ИКС-Медиа» провела 25 апреля в Новосибирске конференцию «ЦОД: модели, сервисы, инфраструктура», которая собрала более 250 делегатов и стала первым столь масштабным мероприятием в Сибири, посвященным обсуждению актуальных вопросов индустрии дата-центров. На следующий день, 26 апреля, состоялось торжественное открытие ЦОДа, построенного в Новосибирской области группой компаний Key Point.

Заместитель министра цифрового развития и связи Новосибирской области Антон Лошаков, выступая на конференции, назвал открытие ЦОДа Key Point эпохальным событием для региона. «Построенный в рекордные сроки с применением преимущественно российских инженерных систем, это первый в Новосибирском регионе дата-центр, который полностью ориентирован на рынок», – заявил он.

Антон Лошаков

По словам А. Лошакова, с ЦОДами в Новосибирске много лет было «непросто». Конечно, ЦОДы есть у федеральных операторов связи и у ряда городских операторов, но все они были созданы компаниями для себя, и лишь часть их ресурсов продается на рынке. Кстати, именно поэтому Минцифры Новосибирской области построило для своих задач два собственных ЦОДа на 200 стойко-мест.

Появление таких объектов, как ЦОД Key Point, подчеркнул замминистра, свидетельствует о том, что ИТ-сообщество вышло на качественно новый уровень. «В Новосибирск приходят инвесторы и строят на продажу ЦОД почти на тысячу стоек. Мы готовы всемерно поддерживать такие проекты», – добавил он.

ЦОДы и регионы

Как известно, российский рынок коммерческих ЦОДов сконцентрирован в столицах. По данным iKS-Consulting, на Москву и Санкт-Петербург приходится 85% этого рынка, или почти 61 тыс. стойко-мест. Из примерно 9 тыс. стойко-мест коммерческих ЦОДов в регионах 1,7 тыс. сосредоточены в Новосибирске. Но ЦОДы здесь в основном небольшие, менее 100 стоек. Объекты большего размера имеются только у четырех компаний: ABC Data center (198 ИТ-стоек), МТС (более 250 стоек), «Ростелеком-ЦОД» (300 стоек) и теперь Key Point (первая очередь ЦОДа – 440 стоек).

Однако дата-центры далеко не всегда бывают коммерческими. Особенно в России. Как отметил Дмитрий Горкавенко, директор по развитию бизнеса iKS-Consulting, если в мире примерно каждая третья ИТ-стойка размещена в коммерческом ЦОДе, то в России каждая пятая. И это если рассматривать типовые 19-дюймовые конструктивы высотой 42–52 юнита. Если же учитывать все возможные конструктивы, которые используются в корпоративных ЦОДах и серверных комнатах для установки ИТ-оборудования, то получится, что лишь каждая десятая стойка в России стоит в коммерческом ЦОДе.

Вместе с тем сектор услуг коммерческих ЦОДов растет быстрее, чем сегмент корпоративных дата-центров, поскольку все большему числу компаний становятся очевидны преимущества их использования. Особенно наглядны эти преимущества при посещении современных высоконадежных ЦОДов, которые все чаще строятся в регионах.

Два лидера

Примером такого дата-центра может служить упомянутый объект ГК Key Point. Это самый большой коммерческий ЦОД в Сибирском регионе и один из самых крупных за пределами Москвы и Санкт-Петербурга. Емкость введенной в эксплуатацию первой очереди ЦОДа составляет 440 ИТ-стоек, общая проектная емкость –


Апрель 2023 г.

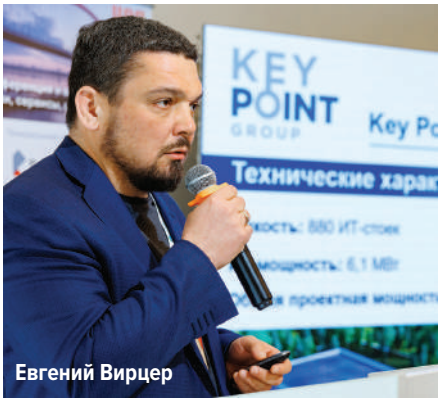

Июль 2023 г.


Февраль 2024 г.

На площадке строительства ЦОДа ГК Key Point в Новосибирской области

880 стоек мощностью 7 кВт. Запуск второй очереди намечен на I квартал 2025 г. Объект уже получил сертификат на соответствие уровню Tier III Constructed Facility, а его услугами начали пользоваться как региональные компании из различных отраслей, так и крупнейшие телекоммуникационные операторы страны, активно развивающие свои ИТ-сервисы в этом регионе.

При создании ЦОДа использовался модульный принцип, в частности, применялись не только внешние, но и внутренние энергомодули, что позволило примерно на три месяца сократить срок реализации проекта, повысив при этом его качество за счет того, что сборка модулей велась в заводских условиях. Как отметил Евгений Вирцер, генеральный директор ГК Key Point, практически все критические инженерные системы



Евгений Вирцер

выполнены на отечественных продуктах. Особо он выделил чиллеры с уникальными характеристиками: температура эксплуатации – до –47°С, что делает их пригодными для экстремально низких температур Сибири.

Второй по емкости в Новосибирске дата-центр (на 300 стойко-мест) принадлежит компании «Ростелеком-ЦОД». Правда, он практически целиком заполнен. Это один из 24 ЦОДов в России, находящихся под управлением «РТК-ЦОД», их общая емкость 20,5 тыс. стойко-мест.

Экономика, безопасность и облако КИИ

Развитие ЦОДов и облачных сервисов, по мнению Дмитрия Панышева, директора по взаимодействию с органами государственной власти «РТК-ЦОД», будут определять три

Дмитрий Панышев

основных фактора: экономика, безопасность и нормативное поле.

Понятно, что, обращаясь к услугам коммерческих ЦОДов, компании и организации существенно снижают капитальные затраты на собственное оборудование и получают возможность гибко масштабировать используемую инфраструктуру с учетом меняющихся потребностей. Например, как рассказал Д. Панышев, ФСС России, перенеся облако из собственной инфраструктуры на ГЕОП, смогла вдвое уменьшить затраты на ресурсы ЦПУ, оперативной памяти и системы хранения данных.

Что касается безопасности и нормативного регулирования, то они тесно связаны. Россия оказалась в пятерке стран, которые за последний год чаще других подвергались кибератакам. По данным, которые привел представитель «РТК-ЦОД», в 2023 г. было совершено 6 тыс. атак только на объекты КИИ, в основном на государственные, промышленные и финансовые организации и предприятия. Ежедневно осуществляется более 170 кибератак на российские компании с целью дестабилизировать их деятельность.

Чтобы усилить защиту от угроз в области ИБ, государство за последние несколько лет разработало целый ряд нормативных документов, в первую очередь для КИИ (к слову, по данным Д. Панышева, из 87 тыс. юридических лиц, работающих в Но-


На одной из дискуссий конференции «ЦОД: модели, сервисы, инфраструктура» в Новосибирске

Рис. 1. Основные отличия облака КИИ (на примере системы «РТК-ЦОД») от типового облака, предлагаемого на рынке ▶

Источник: «РТК-ЦОД»

	Облако КИИ	Облака на рынке
Серверы	РФ	Импорт
Сетевое оборудование	РФ	Импорт
Виртуализация	РФ	Импорт
Операционная система	РФ	Импорт
Платформенное ПО	РФ	Импорт
Система управления инфраструктурой / облачная платформа	РФ	Импорт
Системы хранения данных	РФ	Импорт и РФ
Приложения	РФ	Импорт и РФ
СКУД	РФ	Импорт и РФ
Инженерная инфраструктура ЦОДа	Импорт и РФ*	Импорт и РФ
Оборудование СЗИ	РФ	Импорт и РФ
Средства СКЗИ	РФ	Импорт и РФ

* К инженерной инфраструктуре ЦОДа не применяются требования к импортозамещению

восибирске, 18,7 тыс. являются субъектами КИИ). Требования к объектам КИИ строгие. Так, с 1 сентября 2024 г. на них нельзя будет использовать недоверенные ПАК, приобретенные после указанной даты. (Доверенный ПАК – это ПАК, сведения о котором содержатся в едином реестре российской радиоэлектронной продукции; ПО в составе ПАК должно соответствовать требованиям ПП РФ от 22.08.2022 № 1478, быть включено в единый реестр и при необходимости иметь сертификаты ФСБ и ФСТЭК). А с 1 января 2025 г. начнет действовать полный запрет на использование иностранного ПО на значимых объектах КИИ.

Выполнить все эти требования многим компаниям непросто. Однако они могут использовать предлагаемые «РТК-ЦОД» инфраструктурные (IaaS) и платформенные (PaaS) услуги из «облака КИИ». Эта управляемая облачная инфраструктура, полностью отвечающая требованиям приказа ФСТЭК № 239 (для объектов II категории значимости), сочетает в себе вычислительные мощности, сети и системы хранения данных, обеспечивает заданный уровень надежности и безопасности, а также простое масштабирование. Облако КИИ, развернутое «РТК-ЦОД», практически полностью построено на отечественных продуктах (рис. 1). Импортные решения задействованы только в инженерной инфраструктуре ЦОДа, но к ней жесткие требования по импортозамещению пока не применяются.

Даешь новосибирскую агломерацию ЦОДов!

Эксперты высоко оценивают перспективы развития ЦОДов в Новосибирске. Как показал опрос, проведенный в Telegram-канале «ИКС-Медиа», в числе основных преимуществ региона – хорошая сетевая связность с другими регионами РФ, большое число потенциальных потребителей услуг ЦОДов и облачных сервисов и, наконец, доступность энергетических ресурсов (рис. 2). Короче говоря, три главные составляющие успеха – электричество, связь и клиенты – в Новосибирске есть.

Стоит также отметить наличие высококвалифицированных кадров, ведь Новосибирск – это сибирская столица информационных технологий: в регионе работают более 3 тыс. ИТ-компаний, более 30 тыс. специалистов в сфере ИТ и информационной безопасности.

По прогнозу iKS-Consulting, за ближайшие три года число стойко-мест в коммерческих ЦОДах Новосибирска и области практически удвоится и в 2026 г. составит около 3350 (рис. 3). Для сравнения: это примерно половина всех стоек, насчитывавшихся в 2023 г. в коммерческих ЦОДах Республики Казахстан, которая в 15 раз превосходит сибирский регион по площади и в семь раз – по численности населения. Новосибирск имеет все шансы стать третьей по размеру агломерацией ЦОДов в России после двух столичных.

Александр Барсков
Новосибирск – Москва

◀ Рис. 2. Результаты опроса, проведенного в Telegram-канале «ИКС-Медиа»

Рис. 3. Прогноз роста новосибирского рынка коммерческих ЦОДов, тыс. стойко-мест ▼

ЦОДы Санкт-Петербурга: в ожидании роста

Ужесточение требований к КИИ, углубляющаяся автоматизация производства и необходимость георезервирования ИТ-комплексов – вот факторы, которые могут подстегнуть развитие центров обработки данных в Северной столице.

Под знаком дефицита

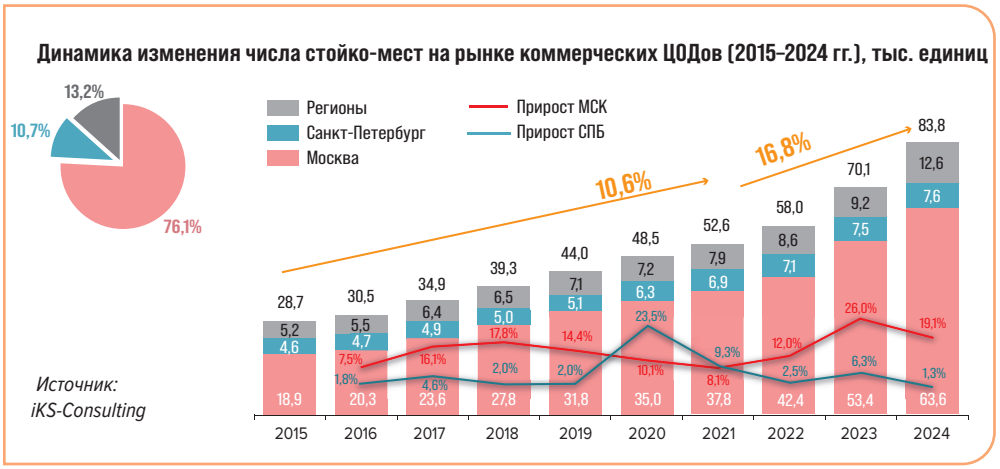
По темпам роста рынок коммерческих ЦОДов Санкт-Петербурга существенно уступает московскому (рис. 1). Что и как может ускорить подъем этого рынка? Этот вопрос стал одним из основных на 7-й конференции «ЦОД: модели, сервисы, инфраструктура», прошедшей в середине июня в Санкт-Петербурге. Мероприятие, организованное «ИКС-Медиа», посетили более 450 специалистов.

В прошлом году рост рынка коммерческих ЦОДов в Санкт-Петербурге, по оценке iKS-Consulting, составил только 6,3%, что примерно в четыре раза ниже, чем в Москве (26%). А в текущем году, как ожидают эксперты, цифра будет еще более скромной – 1,3%. Это значит, что в эксплуатацию запустят всего около 100 стойко-мест – очень-очень мало при нынешних высоких темпах цифровизации.

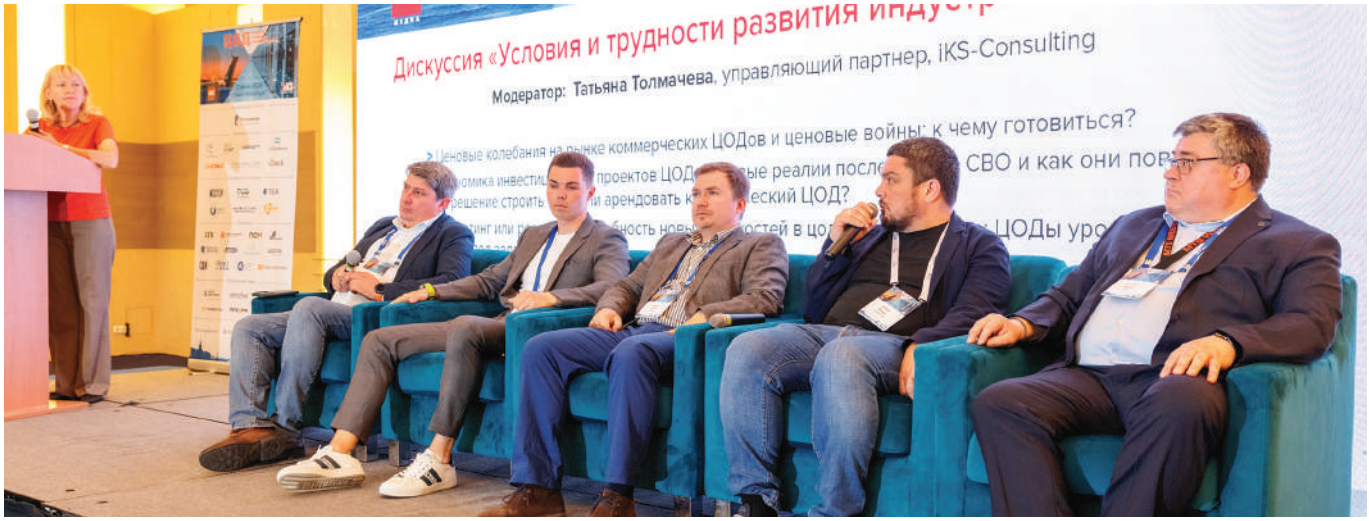
В Москве быстрый рост рынка коммерческих ЦОДов в последние годы был во многом обусловлен дефицитом предложения, рождавшим высокий спрос. Но и сейчас, когда с вводом ряда крупных объектов дефицит преодолен, рост остается двузначным – примерно 20%. По соотношению спроса и предложения рынок Санкт-Петербурга сейчас напоминает московский пару лет назад. Налицо дефицит, особенно на большие (50 и более) пулы стойко-мест. О нем свидетельствуют не только данные аналитиков, но и результаты опроса заказчиков в телеграм-канале «ИКС-Медиа» (рис. 2): на дефицит сетуют 36% опрошенных.

Однако ситуация должна измениться если не в этом, то в следующем году. Так, ГК Key Point на конференции в Санкт-Петербурге объявила о планах построить ЦОД на 1500 стоек, что в 15 (!) раз больше числа всех новых стоек, которые предполагается ввести здесь в строй в 2024 г. Как рассказал основатель ГК Key Point Евгений Вирцер, общая проектная мощность объекта составит 20 МВт, ИТ-мощность – 10,5 МВт. Первую очередь ЦОДа (300 стоек) намечено запустить уже в первой половине 2025 г.

Key Point осуществляет, пожалуй, самую амбициозную программу строительства сети региональных ЦОДов. Во Владивостоке и Новосибирске объекты уже введены в эксплуатацию, идет реализация проектов в Екатеринбурге, Ростове-на-Дону и Махачкале. Стоит отметить, что все ЦОДы своей сети Key Point



◀ Рис. 1. Развитие рынка коммерческих ЦОДов в России



сертифицирует на соответствие требованиям Tier III Uptime Institute.

Сегодня же, пока новые крупные проекты находятся на стадии концепции или проектирования, в коммерческих ЦОДах Санкт-Петербурга насчитывается около 7,5 тыс. стойко-мест. Явный лидер этого рынка – компания Selectel, а пятерка крупнейших операторов – куда также входят «Росэнергоатом» (Xelent), Linxdatacenter, «Ростелеком-ЦОД» и «Миран» – обеспечивает почти три четверти всей емкости (рис. 3).

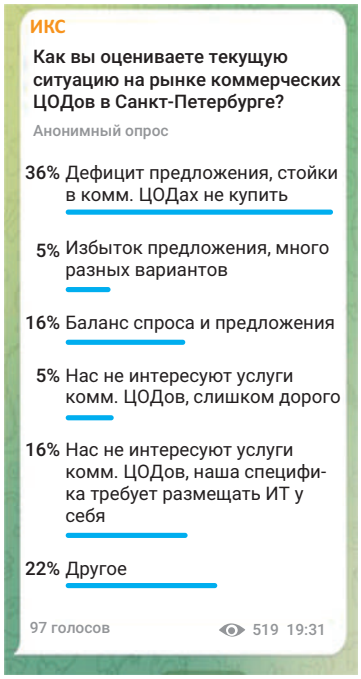
Но далеко не все дата-центры коммерческие. По оценке того же iKS-Consulting, в России в коммерческих ЦОДах размещается только каждая десятая стойка. В Санкт-Петербурге эта доля может быть еще меньше. 22% из опрошенных «ИКС-Медиа» заказчиков вообще не интересуются коммерческими ЦОДами: 6% считают их услуги слишком дорогими, а у 16% специфика требует размещения ИТ-систем на своих объектах (см. рис. 2).

В экономике города, как отмечает ведущий консультант iKS-Consulting Станислав Мирин, много промышленных предприятий (машиностроение, приборостроение, судостроение, радиоэлектроника), которые традиционно используют собственные ЦОДы или серверные комнаты и неохотно идут на аутсорсинг. В то же время финансовые структуры, ритейл, госструктуры, которые более склонны к аутсорсингу, сконцентрированы в Москве.

Но в целом аналитики iKS-Consulting оценивают потенциал развития рынка коммерческих ЦОДов Санкт-Петербурга как «выше среднего». Среди преимуществ: высокая концентрация квалифицированных кадров, надежная телеком-связность с Москвой и Европой, большое количество телеком-операторов. Развитие рынка во многом сдерживается сложностью поиска новых площадок в городе и получения достаточных электрических мощностей.

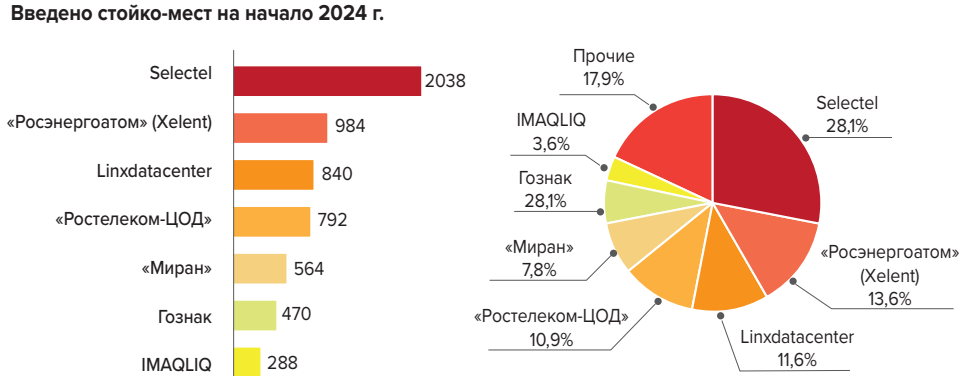
Окна роста

Одним из факторов, которые могут стимулировать развитие рынка дата-центров в Санкт-Петербурге, Дмитрий Панышев, директор по взаимодействию с органами государственной власти компании «Ростелеком-ЦОД», назвал ужесточение требований к объектам критической информационной инфраструктуры (КИИ). Среди таких объектов много промышленных предприятий, далеко не всегда способных удовлетворить эти требования на базе собственных, зачастую устаревших ИТ-комплексов.



Источник: «ИКС-Медиа»

▲ **Рис. 2. Текущая ситуация на рынке коммерческих ЦОДов Санкт-Петербурга (результаты опроса)**



◀ **Рис. 3. Основные коммерческие ЦОДы в Санкт-Петербурге**

Источник: iKS-Consulting

Здесь им могут помочь операторы коммерческих ЦОДов, умеющие выполнять требовании к КИИ.

Другой фактор – увеличивающийся спрос на георезервирование ИТ-комплексов, которое необходимо для обеспечения инфраструктурной безопасности государственных и иных ключевых информсистем. При наличии основной площадки в Москве создание второй площадки в Санкт-Петербурге как раз обеспечит такое резервирование.

Сегодня, в условиях дорогих денег, острой проблемой стало удлинение сроков окупаемости проектов создания ЦОДов. Способствовать решению этой проблемы, как указал Д. Панышев, может субсидирование кредитной ставки при реализации проектов ЦОДов, упрощение доступа к энергетике и включение дата-центров в региональные программы мест приложения труда, что стимулирует девелоперов к развитию инфраструктуры ЦОДов.

Также представитель «Ростелеком-ЦОД» напомнил о мерах поддержки ИТ-отрасли, представленных председателем правительства РФ Михаилом Мишустиным на ЦИПР-2024. Среди этих мер – компенсация до половины затрат на внедрение ключевых классов отечественного инженерного и промышленного программного обеспечения и введение для госкомпаний требований частичного использования облачных сервисов и инфраструктуры коммерческих ЦОДов (для оптимизации расходов госучреждений на ИТ-инфраструктуру и повышения надежности хранения данных).

Кроме того, на индустрию ЦОДов, как отметил Сергей Смирнов, коммерческий директор компании ДКС, серьезное влияние оказывают два глобальных тренда. И первый – повсеместная автоматизация, в том числе внедрение промышленного интернета вещей, – весьма актуален для Санкт-Петербурга и его промышленных предприятий. Второй тренд – внедрение систем на базе искусственного интеллекта. Согласно данным, которые привел С. Смирнов, объем российского рынка ИИ в 2023 г. достиг почти 650 млрд руб., а разработкой ИИ-технологий занимаются более тысячи российских организаций. Оба тренда потребуют дополнительных вычислительных мощностей, а значит, новых ЦОДов.

Новым ЦОДам – новая архитектура?

Возможное изменение подходов к проектированию и построению дата-центров в связи с требованиями, которые предъявляют системы на основе ИИ, – еще одна тема, которая горячо обсуждалась на форуме в Санкт-Петербурге. Тема эта подогрета заявлениями ряда зарубежных провайдеров, в первую очередь гиперскейлеров, о кардинальном пересмотре архитектуры своих ЦОДов для поддержки высокоплотных стоек, необходимых для ИИ-систем. Прежде всего предполагается приоритетное развитие прямого жидкостного охлаждения.

Однако российские эксперты не видят предпосылок для революционного изменения архитектуры ЦОДов, по крайней мере в ближайшее время. Поддержка серверов даже с самыми последними моделями GPU, по их оценкам, потребует стоек на 30–35 кВт. А при разнесении этих серверов по нескольким стойкам с высокоскоростным интерконнектом между ними, как считает Алексей Ерёменко, директор департамента по строительству и эксплуатации ЦОД VK, вполне достаточно и 20 кВт на стойку. Такое тепловыделение снимается традиционными воздушными системами охлаждения. Зачастую даже при типовых архитектурах, рассчитанных на среднюю мощность стойки 7–10 кВт, можно обойтись организацией высокоплотных зон.

Другая острая тема – затруднение доступа к современным технологиям из-за санкций. Но и здесь представители российских ЦОДов и производителей оборудования для них спокойны и уверены в своих силах. По большому счету, за последние два года существенной технологической деградации не отмечается, в стране строятся высоконадежные ЦОДы, отвечающие самым современным мировым требованиям. Несмотря на некоторые сложности с поставками и платежами, наши компании научились ориентироваться в многообразии логистических и финансовых цепочек. И с трека двузначного роста российскую индустрию ЦОДов не столкнуть.

Александр Барсков
Санкт-Петербург – Москва

Как обеспечить доверие к российским ИТ: три стратегии

Николай Носов

Развитие бренда, сертификация совместимости присутствующих на рынке продуктов разных производителей и разработка программно-аппаратных комплексов – основные пути повышения доверия к решениям отечественных компаний.

Требуется бренд

В «лихие» 90-е, когда компьютерный рынок только формировался, появилась новая профессия – покупатель компьютера. Мировые бренды только начинали выходить на российский рынок и большинству соотечественников были не по карману. Покупка же компьютера «красной сборки» представляла собой лотерею. Кто хотел повысить шансы на выигрыш, брал с собой рекомендованного знакомыми специалиста, который прямо у продавца вскрывал системный блок, изучал «начинку» и запускал тесты, попутно заменяя сомнительные детали: диски, порты, видеокарты, а то и браковал весь блок. Причем продавец без возражений выдавал новый. Компаний было много, компьютеры собирались из чего попало, зачастую из комплектующих, снятых с вышедших из строя устройств. В выборе не помогала и реклама, хотя иногда она была честной. Например, я сам купил для банка четыре компьютера российского бренда, постоянно рекламировавшего по телевизору свои изделия под слоганом «Результат превосходит ожидания». Действительно превзошел. Никак не ожидал, что за месяц сгорят три компьютера из четырех.

С введением санкций и уходом из России ведущих мировых вендоров ИТ-оборудования мы как будто снова оказались в тех самых 90-х. На освободившийся рынок хлынули малоизвестные компании, не имеющие сложившейся репутации и истории успеха. В какой-то мере ситуация стала даже сложнее: раньше хотя бы не шла речь о выборе операционной системы – на рынке доминировала Microsoft Windows. А легальность ее приобретения не слишком волновала и окологосударственные структуры. Теперь же приходится искать не только надежное «железо», но и инфраструктурное ПО, причем в условиях резко выросшей стоимости ошибки. Ведь цифровизация сделала практически все отрасли критически зависимыми от ИТ-решений.

Проблема выбора встала остро. Не слишком помогает в поиске Единый реестр российских программ для ЭВМ и БД (ЕРРП). Сейчас в нем более 40 операционных систем, более десятка облачных платформ и систем серверной виртуализации. Множатся другие инфраструктурные решения – гиперконвергентные системы, программно определяемые хранилища, VDI, не говоря уже о прикладных программах. Например, для организации видеоконференцсвязи в ЕРРП представлены около 30 решений.

Клиента, как правило, мало интересуют составные части информационной системы. Главное, чтобы она выполняла свои задачи, работала надежно, а на случай сбоев была сервисная служба, которая сможет вернуть ее в строй. Способов обрести такую систему несколько: обратиться за помощью в выборе к профессиональному «покупателю компьютеров», т.е. опытному интегратору, накопить экспертизу и тестировать продукты самостоятельно либо положиться на новый бренд, который в успешных внедрениях и работе со СМИ только нарабатывает себе репутацию.

Последний вариант для клиента самый простой. Неважно, как появилось решение в портфеле компании: сама она его разработала или купила и интегрировала со своими продуктами, – где нашла и как обучила персонал, как построила экосистему продуктов. Главное, за результат компания отвечает своим именем – брендом.

Расширение портфеля

Стратегия объединения под своим брендом дополняющих друг друга совместимых решений понятна. По этому пути шли многие, в том числе крупнейшие китайские компании, замещающие на своем рынке продукцию мировых лидеров. Они тоже когда-то были маленькими и начинали зачастую с простого копирования западных решений: например, система команд сетевых устройств Huawei до сих пор мало отличается от системы таковых команд у Cisco. Уже потом появились собственные оригинальные разработки, компания стала докупать расширяющие портфель решений готовые бизнесы и стартапы, вышла на рынок ЦОДов. Теперь Huawei производит всё, что нужно для ИТ-инфраструктуры: от чипов и компьютеров до облаков и специализированных платформ для умных аэропортов.

Компаний уровня Huawei в России пока нет, но тенденция к расширению портфеля решений просматривается у многих. Под своим знаменем собирает программные инфраструктурные решения ГК «Астра», добавившая к ОС Astra Linux программный комплекс серверной виртуализации «Брест», облачную платформу VMmanager, систему учета BILLmanager и систему удаленного доступа VDI Termidesk.

Дочка «Ростелекома» компания «Базис» объединяет под своим брендом импортозамещающие решения облачной платформы (Базис. Dynamix Enterprise), серверной (Базис.Dynamix Standard) и контейнерной виртуализации (Базис.Digital Energy), виртуализации рабочих столов (Базис.WorkPlace), а также обеспечивающие работу с ними компоненты безопасности (Базис.Virtual Security), резервного копирования (Базис.Virtual Protect) и систему защиты оконечных устройств (Базис.WorkPlace Security). Особо стоит отметить решения, поддерживающие плавное импортозамещение, возможность параллельной работы отечественной и импортной системы с постепенной миграцией без прерывания бизнес-процессов, что важно для крупных компаний. Таковы, в частности,

С введением санкций и уходом из России ведущих мировых вендоров ИТ-оборудования мы как будто снова оказались в 90-х годах прошлого века

мультиклауд-системы, обеспечивающие параллельную работу в нескольких облаках (например, Базис.Dynamix Cloud Control).

Кроме того, действуя в русле своей стратегии консолидации рынка, «Базис» в начале мая 2024 г. купила компанию РУСТЭК и намеревается использовать приобретенные технологии для развития собственной экосистемы, встраивая их в существующие продукты.

Вендоры аппаратных средств не только расширяют номенклатуру своих изделий, но и начинают выходить на рынки партнеров – поставщиков ПО и услуг. Так, в апреле 2024 г. компания UserGate, специализирующаяся на разработке аппаратных средств обеспечения сетевой безопасности, объявила о запуске в коммерческую эксплуатацию собственного центра мониторинга информационной безопасности (Security Operations Center, SOC), услуги которого будут предоставляться по облачной модели (SOC-as-a-Service). Компания также планирует расширить линейку программных средств сетевой безопасности, в которой к виртуальному шлюзу безопасности добавится решение WAF.

На новые, освободившиеся после ухода зарубежных компаний рынки вышла и группа компаний ICL (Казань). «Текущая ситуация позволяет компании предлагать свои решения в новых отраслях. Это и нефтехимическая промышленность, и розничная торговля, и банки, и промышленность. В 2023 г. мы удвоили, утроили, удесятерили объемы продаж в этих сегментах», – отметил на конференции ICL Partner Connect генеральный директор ГК ICL Евгений Степанов.

Причем казанская компания не только ведет экспансию на новые вертикальные рынки, но и осваивает новые направления. В конце 2023 г. ГК ICL вышла на рынок розничной торговли, предложив линейку компьютеров и ноутбуков собственной разработки под брендом OSIO. Компания стремится стать «российской Huawei», самостоятельно создавая дизайн компьютеров, собирая ноутбуки, рабочие станции и серверы, выпуская печатные платы, разрабатывая коробочное и заказное ПО, занимаясь информационной безопасностью и системной интеграцией.

Сертификация совместимости

Однако в одиночку предложить рынку все необходимые позиции не по плечу даже самым сильным российским брендам. Недостаток собственных ресурсов и экспертизы можно компенсировать построением экосистем, включающих решения сторонних компаний, подтверждая их совместимость сертификационными испытаниями. По этому пути идут многие компании, например «Базальт СПО», публикующая постоянно обновляемые таблицы совместимости.

На совместимость проверяются и продукты основных конкурентов, что расширяет возможности архитекторов разрабатываемых у клиентов систем. В частности, система «Ред Виртуализация» компании «Ред Софт» может использоваться с гипервизором «Базис.Core» от конкурирующего производителя «Базис».

Еще один положительный пример привел на V ежегодной конференции компании UserGate ее менеджер по развитию Иван Чернов: когда один из крупных пользователей UserGate заявил о переходе на операционную систему Astra Linux, компания обеспечила совместимость с ней своего продукта. Недавно был официально выпущен сертификат, который подтверждает совместимость межсетевого экрана UserGate со средой виртуализации, реализуемой ОС Astra Linux и ПК СВ «Брест». ГК «Астра» также подтвердила совместимость своих продуктов с решениями конкурентов UserGate: межсетевым экраном Ideco UTM и виртуальным шлюзом «С-Терра», что расширяет клиентам выбор средств защиты.

К сожалению, не все российские вендоры задумываются об обеспечении совместимости своих решений. «У нас открытая экосистема. С устройствами можно взаимодействовать через открытый API. Использование общепризнанных стандартов и открытых протоколов на нашей стороне позволяет организовать взаимодействие с решениями конкурентов. Однако не все конкуренты готовы к этому и предлагают взаимодействие не по стандарту. Кто тогда должен заниматься доработкой?» – задает риторический вопрос И. Чернов.

Сертификация совместимости решений – общемировая практика, значительно упрощающая работу клиента по построению надежно работающей информационной системы.

▲ **Рис. 1. ПАК «ICL Техно», реализующий кассу самообслуживания**

◀ Рис. 2. Волны импортозамещения в России

Источник: «ИнфоТеКС»

Создание программно-аппаратных комплексов

У бизнеса, как правило, нет возможности, да и желания, заниматься тестированием и разбираться в тонкостях взаимодействия отдельных ИТ-продуктов. Ему нужно решать свои бизнес-задачи, по максимуму перекладывая технические вопросы на вендора или интегратора. Поэтому еще одна стратегия обеспечения доверия пользователей к ИТ-системам – разработка специализированных, заранее интегрированных и подготовленных для конкретных задач программно-аппаратных комплексов (ПАК).

К преимуществам ПАК можно отнести сервисную поддержку комплекса в целом – заказчику не придется разбираться, кто за какую «пуговицу» отвечает, а также эффективность выполнения бизнес-сценариев и снижающую риск человеческих ошибок высокую автоматизацию процессов. И, что важно, не нужно заботиться о совместимости и зрелости задействованных в ПАК отдельных решений.

Направление бурно развивается. Первые записи в разделе «Программно-аппаратные комплексы» появились в ЕРРП только летом 2023 г., а на апрель 2024-го их насчитывалось уже 205. Примерами новых российских инфраструктурных комплексов могут служить ASTRA Infrastructure Starter – ПАК для построения частного облака на продуктах ГК «Астра» и «ICL Техно» или корпоративная платформа баз данных Tantor Xdata, напоминающая Exadata от ушедшей с рынка Oracle, но построенная на продуктах компаний «Тантор Лабс» и «Аквариус».

Целый ряд российских отраслевых ПАК демонстрировался на выставке в рамках конференции ICL Partner Connect: для медицины – мобильное рабочее место медсестры, для ритейла – кассы самообслуживания (рис. 1), и даже ПАК для изучения иностранных языков в вузах от «Ред Софт» и «ICL Техно».

Волны импортозамещения

В России, по словам советника генерального директора «ИнфоТеКС» Евгения Генгриновича, можно насчитать четыре волны импортозамещения (рис. 2). Первая началась после введения против нашей страны санкций в 2014 г. Правда, в ту пору импортозамещение чаще всего заключалось в наклейке своих шильдиков на изготовленное в Юго-Восточной Азии оборудование.

Во время второй волны, примерно с 2018 г., российские вендоры стали заниматься крупноузловой сборкой из готовых комплектующих. По сравнению с переклейкой шильдиков – большой прогресс. Пусть узлы собирались за рубежом, но их выбор, тестирование и ответственность за итоговое решение оставались за российским вендором.

Сильным толчком к импортозамещению послужили события февраля 2022 г., ужесточение санкций и уход с рынка зарубежных вендоров. Изменения коснулись всех, импортозамещением озаботились не только государственные, но и не попавшие под санкции коммерческие структуры.

Особенно обострились вопросы импортонезависимости электронной компонентной базы. После присоединения к санкциям Тайваня выпуск российских процессоров на неопределенное время остановился, а перспективы освоения производства современных микропроцессоров в России выглядят туманными.

Поставка крупных узлов усложнилась, но в целом зарубежная микроэлектроника осталась доступной. Это позволило заняться дизайном и производством российских аппаратных решений из мелких комплектующих.

Импульсом для четвертой волны во многом стали вопросы кибербезопасности, прежде всего объектов КИИ, защита которых попала под пристальное внимание регуляторов. Безопасность на них должна обеспечиваться путем применения доверенных программно-аппаратных комплексов, включающих российские аппаратные и программные средства. Причем российские ПАК востребованы и на менее критичных объектах.

Ставка на программно-аппаратные комплексы не исключает других путей повышения доверия к российским ИТ-решениям и может сочетаться с созданием сильного бренда и экосистем совместимых между собой продуктов. Время уникальное, явных лидеров мало, шансы есть у всех. ИКС

Ставка на экосистему

О формировании устойчивой экосистемы с предсказуемостью технических решений и сервиса на всех этапах жизненного цикла ЦОД рассказывает Роман Шмаков, первый заместитель генерального директора по рынку «ИТ-решения» компании Systeme Electric.

– Какие тенденции вы видите на мировом рынке цодостроения? Каковы наши национальные особенности?

– Общаясь с коллегами из других стран, отмечаем продолжающуюся тенденцию «озеленения» и цифровизации ЦОД. Эти вещи неразрывно связаны. Улучшение энергоэффективности, экологичности, устойчивости ЦОД – все это обеспечивается в первую очередь за счет цифровизации. Все больше элементов ЦОД становятся «умными», улучшается их связность, повышается сквозная цифровизация инфраструктуры, углубляется интеграция с программными платформами. ЦОД становятся все более софтверными. Если раньше в них доля ПО (относительно аппаратного обеспечения) была низкой, то сейчас она увеличивается – с точки зрения как технологий, так и бюджетов.

Если говорить о российском рынке, то на нем, безусловно, сказываются геополитические вызовы. Поэтому важно, чтобы производители создавали устойчивую экосистему. Цодостроители (системные интеграторы) хотят иметь технологии понятные и надежные и по техническим параметрам, и по логистике, чтобы была уверенность: заложенные в концепцию, в проект продукты будут изготовлены и поставлены в требуемые сроки. Здесь важны глубина присутствия производителя, уровень поддержки, гарантия продолжения поставок в будущем по мере развития ЦОД.

В России также видим устойчивый тренд к повышению значимости сервиса. У нас сервисное подразделение развивается очень активно. Сервисы проектирования, модернизации, замены оборудования (многие ЦОД в России построены более 10–15 лет назад) все более востребованы. Плюс опять же цифровизация: заказчики хотят лучше понимать, что происходит на площадке, требуют более детального мониторинга, более эффективного управления.

– В 2022 г. ситуацию на российском рынке решений для инженерной инфраструктуры вы охарактеризовали как «Дикий Запад». Далеко ли нам еще до стабилизации?

– Как ни удивительно, но «Дикий Запад» с непрозрачными цепочками поставок и процессами производства и сервиса у отдельных участников рынка сохраняется. Первая волна прошла, многие поставщики уже отказались от работы на рынке ЦОД. Одни по экономическим причинам: торговать с минимальной маржой и выполнять просто функции логиста рискованно, особенно в текущей турбулентной ситуации. Другие поняли: рынок относительно небольшой и очень конкурентный. В основном это китайские производители, которые вышли на рынок в режиме тестирования.

Но возникла вторая волна: появились компании, которые раньше и не собирались работать в России. Создан целый пласт альянсов: производитель, приходя на наш рынок, находит партнеров и дальше работает с рынком через локальные компании. Это, в частности, и не позволило ситуации стабилизироваться окончательно.

При этом на фоне всех названных процессов рынок самообучился. Набив определенное число шишек, участники рынка – системные интеграторы, строители, инжиниринговые компании – научились работать со множеством производителей, продуктов, каналов поставки. Заказчики стали более разборчивыми, гораздо более осознанно подходят к выбору решений. В итоге, конечно, «дикие» игроки вымрут, останутся цивилизованные, которые хотят работать на рынке вдолгую.

– С учетом дороговизны денег многие проекты поставлены на паузу. В результате через пару лет может возникнуть острый дефицит стойко-мест в коммерческих ЦОД. Что способно изменить ситуацию? Как вендор может помочь заказчикам повысить рентабельность проектов?

– Вопрос действительно стоит остро. Сейчас, когда усложнились цепочки поставок и доступность технологий стала ниже, экономические показатели проектов «поплыли». Раньше на рынок приходили девелоперы, которые до того не занимались ЦОД, и ситуация позволяла им быть немного дилетантами: экономический люфт проектов допускал небольшие ошибки, не самую высокую эффективность. Сейчас люфтов «на дилетантство» не осталось. Даже профессиональные игроки, чтобы выдержать жесткие экономические параметры проектов, вынуждены гораздо более пристально отслеживать все критерии, заниматься ручным управлением проектами, где-то даже микроменеджментом.

Мы как производитель помогаем в ряде моментов. Цена далеко не всегда самое главное, хотя, конечно, стараемся быть конкурентными и в этом плане. Но важнее ценность решения. Помогаем оптимизировать затраты и исключать ошибки с помощью интеллектуальных услуг нашего консалтингового подразделения, которые охватывают все стадии жизненного цикла: проектирование, строительство, тестирование, запуск в работу, эксплуатацию и модерниза-

цию. Это положительно влияет на экономическую эффективность проектов.

– Насколько завершено формирование продуктового портфеля Systeme Electric?

– Год назад я говорил, что мы завершаем формирование нашего комплексного портфеля. Сейчас могу с уверенностью сказать, что мы это сделали. Недавно прошел Инновационный Саммит 2024, где мы презентовали весь портфель решений. Одна из самых важных новинок – Excelente VX, модульный ИБП с высокой эффективностью, который предназначен для средних и больших ЦОД.

Существенно расширили предложение стоечных решений и блоков распределения питания (БРП). Отдельно отмечу, что наши БРП существенно отличаются от других предложений на рынке. Мы долго их готовили, много занимались софтом, микрокодами, схемотехникой, и в результате получились отличные продукты, причем во всех нишах: базовые, с мониторингом, с мониторингом и управлением.

Обновили системы охлаждения: расширили модельный ряд, дополнили ходовыми моделями. Есть варианты для высокоплотных систем, что особенно актуально в связи с интересом к искусственному интеллекту. Прорабатываем варианты жидкостного охлаждения.

И «вишенка на торте» – наша система мониторинга и управления. Она обратно совместима с решениями APC. В России большая инсталлированная база систем APC, покинувшей рынок, и теперь заказчики получили возможность модернизировать их, не заменяя, а дополняя. По возможностям масштабирования и интеграции наше решение превосходит продукты APC. Наша команда долгое время работала под брендом APC и использует лучший мировой опыт и экспертизу для собственных разработок, отвечающих требованиям российского рынка. Система интегрируется со SCADA-системами зданий, может быть частью общей платформы управления инженерной инфраструктурой объекта в целом – это важно, когда ЦОД является частью здания.

– Systeme Electric, как в свое время покинувший Россию ведущий мировой производитель, предлагает комплексное решение для инженерной инфраструктуры ЦОД. Как показало исследование, проведенное Systeme Electric совместно с iKS-Consulting, в комплексном решении продуктовая составляющая не на первом месте. Важнее сервисы, экспертиза. Как вы это прокомментируете?

– Результаты исследования подтвердили нашу гипотезу, наш опыт в отдельных проектах. Заказчики готовы поступиться какими-то техническими параметрами, если понимают, что ценность работы с производителем, который предлагает экосистему, гораздо выше, чем, например, лишние полпроцента КПД отдельного ИБП. Поэтому мы сделали акцент на развитие комплексной экосистемы, это наша стратегия.

Сервисы, о которых я уже упоминал, – важная часть этой стратегии. Сервисы становятся более «умными», что обусловлено как развитием продуктов, – которые «на борту» имеют широкие возможности для интеграции в единую систему, – так и развитием ПО, которое позволяет эффективно управлять инфраструктурой. Все более востребованы и сервисы, связанные с техническим обслуживанием и ремонтом, благодаря которым заказчики могут управлять различными регламентными работами, ремонтом с привлечением цифровых инструментов, в том числе предиктивной аналитики с элементами искусственного интеллекта. Простой пример: датчик, который замеряет биение подшипника вентилятора чиллера или кондиционера, помогает прогнозировать выход из строя устройства. Он формирует предупреждения, подсказывает, когда и какое провести обслуживание, что поменять.

– Каковы сегодня основные векторы развития отечественных производителей, вашей компании?

– Важнейший вектор – локализация. Но не только для попадания в реестры регуляторов, а для того, чтобы обезопасить себя как производителя от копирования продуктов и других рисков. Чем больше локальных работ и компонентов, тем меньше риск, что какие-то комплектующие не доедут из зарубежных стран. Это тоже часть нашей стратегии. Увеличиваем и будем увеличивать долю локального производства – и на наших собственных, и на партнерских производственных площадках.

Серьезный упор делаем на локализацию интеллектуальных составляющих, НИОКР, конструкторские разработки, написание ПО и микрокодов. У нас своя софтверная компания, которую мы зарегистрировали в Минцифры.

Другой вектор – совершенствование управления логистическими и финансовыми цепочками. Это тоже ответ на существующие реалии. Кроме того, мы объединяем усилия с партнерами – технологическими лидерами в различных областях – для совместных разработок и масштабирования производства, при том, что курс на локализацию остается неизменным. Например, «Систэм Электрик» создала совместное предприятие с Delixi Group, одним из лидеров китайского рынка в области производства оборудования для конечного распределения.

– Кого видите основным конкурентом на рынке решений для инженерной инфраструктуры ЦОД?

– В комплексных решениях реальных конкурентов не вижу совсем. А вот в отдельных нишах они есть, например, ряд российских компаний, которые давно и небезуспешно занимаются производством или сборкой ИБП.

Как мы уже обсуждали, комплексный подход – это не просто выпуск еще одного продукта. Это экспертиза, инженерная команда, сервисы. Важно также, чтобы компания была «заточена» под комплексные проекты. Это логистика, управление финансами и др. – надо предусмотреть массу нюансов, чтобы предложение действительно было комплексным, а не просто набором продуктов, которые функционально охватывают все области.

Мы изначально сделали ставку на комплексный подход, и он себя оправдывает. Это подтверждают и отзывы клиентов, и результаты бизнеса.

ЦОД-прогнозы 2024

Окончание. Начало см. «ИКС» №2'2024, с. 24.

Дуглас Доннеллан, аналитик-исследователь,
Энди Лоуренс, исполнительный директор по исследованиям,
Дэниел Бизо, директор по исследованиям,
Макс Смолакс, аналитик-исследователь,
Жаклин Дэвис, аналитик-исследователь,
Джон О'Брайен, старший аналитик-исследователь,
Uptime Institute Intelligence

Растущие требования к охлаждению серверных чипов заставят внедрять технологии DLC, датацентричное управляющее ПО будет применяться все шире, а появление кампусов гиперЦОДов повысит спрос на инфраструктурное оборудование и цены на colocation и облачные услуги.

Прогноз 3. Прямое жидкостное охлаждение не повысит эффективность радикально

Все больше операторов ЦОДов и поставщиков оборудования считают, что в ближайшие несколько лет системы прямого жидкостного охлаждения (Direct Liquid Cooling, DLC) получат широкое распространение. Недавно поставщики ИТ- и инженерного оборудования совместно с рядом крупных операторов занялись развитием коммерческих систем DLC в ответ на растущие требования к охлаждению серверных чипов.

Основным преимуществом технологии DLC ее адепты называют повышение энергоэффективности ЦОДов. В частности, тепловые характеристики жидкостей, гораздо более привлекательные по сравнению с воздухом, позволят снизить потребление электроэнергии и воды в системах охлаждения, а также увеличить возможности круглогодичного естественного охлаждения (фрикулинга) в некоторых климатических условиях. Это, в свою очередь, даст возможность повысить эксплуатационную устойчивость ЦОДа.

Однако многие операторы, планирующие в ближайшие несколько лет внедрять системы DLC, в первую очередь, скорее всего, будут уделять внимание быстроте и простоте их установки, интеграции в существующую инфраструктуру и поддержанию ее отказоустойчивости, а не достижению максимальной энергоэффективности.

Использование DLC в критически важных инфраструктурах потребует серьезного изменения подходов к проектированию систем охлаждения и их эксплуатации, а отраслевые практики еще только предстоит наработать. Многие операторы ЦОДов сочтут существующие системы DLC неэкономичными для своих задач, что замедлит их внедрение в отрасли в целом.

Охлаждение в смешанном режиме

Операторам ЦОДов придется в течение длительного времени совмещать на своих объектах системы с жидкостным и воздушным охлаждением. Во многих случаях это будет означать, что инфраструктура охлаждения будет использоваться такими системами совместно. Но DLC будет внедряться не только в ЦОДах, в которых установлены чиллеры, но и на других объектах, где жидкость для охлаждения не применяется.

В гибридных средах энергоэффективность DLC будет ограничена требованиями к температуре приточного воздуха (для оборудования воздушного охлаждения), что ограничит работу при более высоких температурах – а значит, снизит эффективность использования электроэнергии и капитальных затрат на системы DLC.

DLC позволяет отказаться от большей части серверных вентиляторов и снижает требования к характеристикам охлаждающего воздушного потока, но вклад этого в повышение общей энергоэффективности инфраструктуры трудно оценить количественно, поскольку мощность ИТ-вентиляторов обычно не отслеживается – она скрыта в показателях общей ИТ-нагрузки.

Потребуются годы, чтобы установки DLC достигли таких масштабов, при которых их использование в качестве стандартного подхода к охлаждению в ЦОДах станет оправданным.

Скрытые температурные компромиссы

Те же тепловые свойства жидкостей, которые позволяют снизить энергозатраты, могут

Печатается с разрешения Uptime Institute.

послужить повышению производительности систем охлаждения. Даже если есть возможность выбора, некоторые операторы предпочитают подавать в системы DLC жидкость более низкой температуры.

Низкая температура жидкости в установке позволяет уменьшить ее расход для обеспечения той же холодопроизводительности, что снижает нагрузку на трубопроводы и насосы, включая узлы распределения охлаждающей жидкости в системах DLC. Использование более холодной жидкости также упрощает планирование и проектирование ЦОДов, гарантируя возможность удовлетворения будущих потребностей серверной техники. Требования к температуре охлаждающей жидкости будут только ужесточаться по мере прогресса в микросхемах серверов.

ИТ-оборудованию тоже «выгодны» более низкие температуры. У процессоров, например, при более низких температурах уменьшаются потери из-за накопления статического электричества, и сэкономленную энергию можно направить на другие цели. Это особенно ценно, когда оператор хочет добиться максимальной производительности при минимальных затратах, что часто важно при высокопроизводительных вычислениях, в частности, при обучении систем ИИ. Работа серверов при более низкой температуре также уменьшает частоту отказов компонентов в целом.

Преимущества низких температур для инженерных и ИТ-систем часто перевешивают преимущества более «бережливой» инфраструктуры охлаждения. Внедрение DLC, скорее всего, будет связано по большей части с инвестициями в повышение производительности охлаждения и ИТ, а не в повышение эффективности.

DLC – это замена не только теплоносителя

При всех потенциальных преимуществах переход на DLC создает проблемы при проектировании, обслуживании и эксплуатации систем обеспечения отказоустойчивости. Сохранение возможности обслуживания без прерывания работы или поддержание отказоустойчивости в некоторых системах DLC может оказаться непрактичным. Кроме того, в системе DLC время работы охлаждающих пластин в случае сбоя, как правило, не превышает минуты (из-за небольшого объема охлаждающей жидкости), а при высоких температурах перегрев серверов может произойти всего за несколько секунд. В результате переход на DLC может потребовать пересмотра схем обеспечения отказоустойчивости инфраструктуры дата-центров.

Необходимо будет пересмотреть процедуры закупок, ввода в эксплуатацию, технического обслуживания и эксплуатации ЦОДов, поскольку DLC нарушает существующее сегодня разделение функций инженерной и ИТ-инфраструктуры. При использовании воздушного охлаждения оборудование четко разделено между инженерами и айтишниками. Для жидкостного охлаждения такой четкой границы нет. Перераспределение обязанностей заставит инженерные и ИТ-команды сотрудничать гораздо более тесно. Все это потребует значительных усилий и времени.

В долгосрочной перспективе (10 лет и более) системы DLC, скорее всего, возьмут на себя обслуживание большей части ИТ-нагрузки – по мере того как работы по стандартизации, реальный опыт использования систем DLC и продуманные рекомендации будут воплощаться в новых, более надежных продуктах и передовых практиках.

В ближайшей перспективе при разработке бизнес-плана для внедрения DLC приоритетное внимание, скорее всего, будет уделяться повышению производительности ИТ-оборудования и простоте внедрения с использованием общей инфраструктуры охлаждения. Важно отметить, что более низкие температуры подаваемой жидкости и использование чиллеров упростят задачу обеспечения отказоустойчивости. Поскольку многие операторы ЦОДов считают, что повышение производительности и использование гибридных сред эксплуатации сегодня более актуальны для бизнеса, чем задачи перехода на фрикулинг и повышения экологичности, решение последних, видимо, придется немного отложить.

Преимущества более низких температур для инженерных и ИТ-систем часто перевешивают преимущества более «бережливой» инфраструктуры охлаждения

Прогноз 4. ПО дата-центров станет более интеллектуальным

Большинство владельцев и операторов ЦОДов в настоящее время используют системы управления зданиями (BMS) и/или ПО для управления инфраструктурой дата-центров (DCIM) в качестве основных инструментов для управления объектами. Эти инструменты важны, но обладают ограниченными аналитическими средствами и возможностями автоматизации, поэтому мало что дают для повышения эффективности работы инженерной инфраструктуры.

Специалисты Uptime Intelligence давно утверждают, что системы управления ЦОДами должны развиваться в направлении обеспечения большей автономии. Впервые модель зрелости управления ЦОДами была предложена нами в 2019 г. Сегодня наметился выход на уровни 4 и даже 5 (табл. 1), хотя с оговоркой: одной системы DCIM, скорее всего, недостаточно для полноценной реализации соответствующих возможностей. Ее нужно объединить с новым поколением инструментов, ориентированных на работу с данными.

Дата-центричное ПО управления способно:

- повысить эффективность систем электропитания и охлаждения – благодаря автоматизи-

рованной настройке оборудования, а также выявлению неэффективного или неисправного оборудования;

- улучшить техническое обслуживание – за счет анализа и прогнозирования состояния отдельных аппаратных компонентов;
- выявить нехватку ресурсов – в результате тщательного анализа всех характеристик ЦОДа, а не только метрик высокого уровня;
- исключить человеческие ошибки – благодаря более высокой степени автоматизации либо автоматически генерируемым рекомендациям для персонала;
- улучшить управление навыками – за счет анализа и систематизации навыков наиболее опытных сотрудников.

Внедрение дата-центричных инструментов управления инфраструктурой заставит ее владельцев и операторов осознать важность качества данных

Это все про данные

ЦОДы полны различных датчиков, которые могут служить источником ценной оперативной информации. За последние несколько лет появились новые платформы, которые упрощают обработку и анализ данных. Это позволяет крупным организациям разрабатывать собственные приложения, включая модели машинного обучения, использующие данные об оборудовании.

Не все модели машинного обучения требуют больших вычислительных ресурсов, обширных наборов данных и длительного времени обучения. На самом деле многие модели, применяемые сегодня в ЦОДах, невелики и относительно просты. Как обучение, так и использование его результатов могут выполняться на серверах общего назначения, и не всегда требуется объединять данные с нескольких площадок – обученной локально модели часто бывает достаточно для получения необходимых результатов.

Табл. 1.
Модель зрелости управления ЦОДами ▼

Уровень зрелости	Описание	Операционная эффективность
1	Базовый мониторинг обеспечивается с помощью ПО поставщика оборудования и систем BMS	Низкая
2	Используется ПО для мониторинга параметров рабочей среды и энергопотребления оборудования. Возможна базовая настройка оборудования (например, систем охлаждения) в соответствии с требованиями	Низкая
3	ПО способно отслеживать характеристики оборудования, его местоположение и состояние. Данные об энергопотреблении и рабочей среде используются для снижения рисков и потерь	Средняя
4	Для прогнозирования и управления сервисами в режиме, близком к реальному времени, задействуется машинное обучение. Базы данных DCIM углубленно анализируются с помощью ИИ	Средняя
5	Интегрированное ПО управления на основе ИИ регулирует «поведение» ЦОДа и обеспечивает оптимальное использование ресурсов в соответствии с целями, правилами и требованиями к сервисам на протяжении всего жизненного цикла	Высокая

Новые инструменты – новые задачи

Внедрение дата-центричных инструментов управления инфраструктурой заставит ее владельцев и операторов осознать важность качества данных. Нельзя доверять выводам моделей машинного обучения, если нет доверия исходным данным. Поэтому потребуется дополнительная работа по стандартизации и очистке хранилищ оперативных данных. В некоторых случаях операторам ЦОДов придется нанимать аналитиков и специалистов по обработке данных для совместной работы со службой эксплуатации инженерной и ИТ-инфраструктуры.

Сбор данных в больших масштабах неизбежно потребует расширения сетей их получения внутри ЦОДов, в том числе беспроводной сети. Это даст киберпреступникам потенциально более широкие возможности для атак. Таким образом, кибербезопасность станет важным фактором при любом оперативном внедрении ИИ и ключевым риском, которым необходимо будет постоянно управлять.

Эволюция неизбежна

В настоящее время инновациями в области ИИ и аналитики управления ЦОДами занимаются в основном стартапы и не очень известные поставщики ПО. Лишь немногие разработчики BMS и DCIM интегрировали машинное обучение в свои основные продукты.

Скорость массового внедрения подобных инструментов будет зависеть от того, насколько это внедрение будет простым. В конечном счете отрасль придет к определенному набору процессов и политик, направленных на извлечение пользы из данных, которые получают от оборудования.

Прогноз 5. ГиперЦОДы изменят карту дата-центров

В ответ на растущий спрос на вычислительные ресурсы и хранилища данных в разных частях света создаются масштабные кампусы гиперЦОДов. Хотя большинство таких проектов имеют мощность ниже 1 ГВт, некоторые рассчитаны на гигаваттную мощность. (Эксперты Uptime считают, что приставка «гипер» применима к объектам мощностью от 100 МВт и выше.) Эти цодовские города огромных размеров предназначены в основном для предоставления услуг colocation, их не надо путать с гигантскими объектами гиперскейлеров.

Анализ 35 недавних проектов создания кампусов гиперЦОДов для colocation по всему миру дает среднюю планируемую мощность более 400 МВт. Но эта цифра зависит от региона: в Азиатско-Тихоокеанском регионе количество проектов наибольшее, но средняя мощность одного кампуса –

менее 200 МВт, в то время как в Северной Америке она превышает 600 МВт (табл. 2).

Если бы все эти проекты были построены и работали хотя бы на половину проектной мощности, на их долю приходилось бы около 51 ТВт·ч потребленной энергии в год. По текущим оценкам, ежегодное потребление энергии ЦОДами составляет 200–400 ТВт·ч.

Кампусы гиперЦОДов для colocation

Согласно опубликованным на данный момент планам, такие кампусы будут состоять из гиперЦОДов, расположенных на одном участке площадью в миллионы квадратных метров. В одном кампусе в зависимости от его размера и масштабируемости могут размещаться несколько поставщиков услуг colocation.

Дорогостоящая инфраструктура – широкополосные оптические подключения, электрические трансформаторные подстанции, системы генерации и хранения возобновляемой энергии – может использоваться несколькими арендаторами ЦОДов совместно.

Объем инвестиций в проекты такого масштаба часто требует создания консорциума инвесторов, в который могут входить заинтересованные стороны всей экосистемы, связанной с ЦОДами. Здесь ключевую роль призваны сыграть гиперскейлеры: их участие стимулирует и гарантирует спрос, а также обеспечивает доверие, финансирование, подключение и экспертные знания.

В большинстве случаев в проект вовлечены один или два ведущих оператора, оптовые colocation-компании или гиперскейлеры. При этом ожидается, что более мелкие операторы также будут использовать ресурсы кампуса.

Кампусы гиперЦОДов будут обеспечены резервируемыми высокоскоростными оптическими соединениями с другими крупными агломерациями ЦОДов. Их будут стараться размещать там, где негативное влияние на окружающую среду будет минимальным.

Подобные проекты, разработанные с учетом целей низкоуглеродной или безуглеродной энергетики, могут предусматривать заключение контрактов на закупку электроэнергии из возобновляемых источников, а также установку собственных средств такой генерации. Это может быть солнечная, ветровая, геотермальная и даже ядерная энергия. Кроме того, в таких проектах часто предусматривается использование микросетей для управления ресурсами генерации как на самой площадке, так и за ее пределами.

Вот некоторые характеристики и возможности кампусов гиперЦОДов:

- оптимизация энергопотребления. Коэффициент PUE, как правило, не выше 1,4, а во многих местах ближе к 1,2;

Регион	Общая подведенная мощность, МВт	Число проектов	Средняя мощность, МВт	Общие расходы, $ млн
Северная Америка	6210	10	621	45 000
Азиатско-Тихоокеанский (без КНР)	3832	21	182	11 628
Европа, Средний Восток и Африка	750	2	375	6400
КНР	500	1	500	4890
Латинская Америка	450	1	450	400
Всего (по миру)	11 742	35	335	68 318

Учтены проекты, о которых объявлено в 2021 г. и позднее, без объектов гиперскейлеров.

▲ Табл. 2. Проекты создания кампусов гиперЦОДов (мощностью 100 МВт и выше)

- применение модульных конструкций во внутренних и внешних пространствах для быстрой реконфигурации;
- использование систем управления на основе ИИ для оптимизации мониторинга, производительности и доступности ресурсов ЦОДов;
- поддержка высокоплотных высокопроизводительных серверов и графических процессоров (GPU) для запуска моделей искусственного интеллекта. Скорее всего, это потребует жидкостного охлаждения.

Влияние на индустрию ЦОДов

В наибольшей степени распространение кампусов гиперЦОДов затронет четыре области:

- **Карта ЦОДов.** По мере создания кластеров ЦОДов будут формироваться новые центры притяжения заказчиков. Это, вероятно, изменит стоимость услуг colocation, облачных вычислений и телеком-услуг.
- **Цепочки поставок.** Создание кампусов гиперЦОДов повысит спрос на все инфраструктурное оборудование (который и так высок) и позволит операторам осуществлять более масштабное строительство, что, в свою очередь, будет способствовать повышению уровня автоматизации и привлечению инвестиций.
- **Экологичность.** Новые объекты ориентируются на использование низкоуглеродных источников энергии. Постоянно растущий спрос на ИТ-ресурсы оправдывает крупномасштабные инвестиции и массовые инновации, а кампусы ЦОДов станут центрами развертывания микросетей, аккумуляторов с длительным временем автономии и систем возобновляемой энергии.
- **Отказоустойчивость.** Кампусы гиперЦОДов (и их системы коннективности) наряду с новыми ЦОДами в небольших городах и edge-ЦОДами сформируют более устойчивую и надежную цифровую инфраструктуру национального и международного уровня.

Эксперты Uptime считают, что приставка «гипер» применима к объектам мощностью от 100 МВт и выше

Полный текст статьи читайте на www.iksmedia.ru

Alcon DC Nord – технопарк и ЦОД премиальной надежности на Соколе

Один из девелоперов на столичном рынке недвижимости Alcon Group строит в составе технопарка на севере Москвы 20-мегаваттный ЦОД уровня Tier IV. Подробнее о проекте – Артем Панин, заместитель генерального директора компании.

– Что будет представлять собой ваш центр обработки данных?

– Строящийся объект расчетной мощностью 21,3 МВт располагается на севере Москвы, в районе метро «Сокол» (3-й Балтийский пер., вл. 5). В него входят собственно ЦОД (20 МВт), офисный комплекс и подземная парковка. В здании ЦОДа шесть этажей. Первые два – технические, где, в частности, будет установлено энергетическое оборудование. С третьего по шестой – помещения под информационные технологии и связь (машинные залы), по три на этаже: всего 12 машзалов, 1968 стоек средней мощностью по 5 кВт.

Хочу подчеркнуть, что наш проект не просто ЦОД, а технопарк, в составе которого реализован ЦОД. Он имеет статус приоритетного проекта города Москвы и официально называется Инновационный центр «Технопарк «Алкон Север». Статус технопарка дает ряд преференций как нам, так и нашим будущим клиентам. Для нас как управляющей компании технопарка это сниженные налоги на прибыль и на землю, освобождение от налога на имущество. Для резидентов также предусмотрены налоговые льготы.

Будущие клиенты технопарка получат возможность в приоритетном порядке арендовать помещения для резервных офисов и других целей, причем рядом с «любимым железом» – айтишникам это важно. Такая концепция позволяет сделать технопарк настоящим центром ИТ-развития, а не только сугубо технологической площадкой для размещения оборудования.

Отмечу территориальные преимущества объекта. Это так называемый Ленинградский коридор, отличная транспортная доступность. Можно быстро добраться до Шереметьево. Кроме того, у нашего объекта прекрасные возможности для организации связности с другими ЦОДами – в радиусе 10 км находится большинство основных московских ЦОДов. На небольших расстояниях расположено много офисных центров, в том числе те, где размещаются ведущие ИТ-компании. Им будет удобно организовать взаимодействие своих серверных комнат или edge-ЦОДов с нашим дата-центром, например, для задач резервирования.

– В какой стадии сейчас находится проект?

– На данный момент (середина июня 2024 г.) ведется разработка рабочей документации и одновременно идет строительство – заливается фундаментная плита.

Ввод в эксплуатацию первого этапа намечен на II квартал 2026 г. Замечу, что мы сразу будем делать всю инфраструктуру, прокладывать слаботочные линии, силовые кабели, вентиляцию, все коммуникации, выполнять всю отделку в технических помещениях и помещениях общего пользования и т.д. А вот крупноузловое и капиталоемкое оборудование (ДГУ, чиллеры, ИБП и пр.) будем устанавливать по этапам. Намечено три этапа, каждый предполагает ввод в эксплуатацию стойко-мест с инженерными системами суммарной мощностью по 7 МВт.

Сроки реализации второго и третьего этапа – исключительно коммерческое решение. На первом этапе вводим 653 стойко-места. Далее все будет определяться спросом. Если он высокий, можем оперативно закупить все инженерное оборудование и ввести в эксплуатацию весь ЦОД.

– С оборудованием сейчас не очень просто. На каких поставщиков ориентируетесь?

– Стараемся минимизировать геополитические, санкционные риски. Если есть возможность, выбираем оборудование российского поставщика с максимальным процентом локализации. В случае с ИБП это сделать проще, выбор есть. С ДГУ сложнее, подходящие двигатели у нас не делают. Но проблем с закупкой и поставкой ДГУ быть не должно.

По охлаждению ситуация пока следующая. Ориентируемся на чиллеры известного европейского производителя. Но есть и варианты российского производства, их тоже не сбрасываем со счетов, тестируем, готовимся к ухудшению условий. Ситуацию немного осложняет то, что нам нужны мощные чиллеры, по 1,5 МВт, плюс у нас жесткие требования по уровню шума и габаритам. Не многие компании производят такие аппараты, выбор сужается.

– Кто вам помогает проектировать и строить объект, кто будет его эксплуатировать?

– Генпроектировщик и генподрядчик – мы сами. С рынка берем только те компетенции, которых у нас нет. Для этого в проект включена команда опытных профессионалов от компании 3-BS, ранее работавших в международных и российских проектах строительства ЦОДов компании HPE. Они выполняют функции технологического консалтинга и управления проектом в части специализированных инженерных систем: энергетика, холодоснабжение, слаботочка. Также в команду проектировщиков входят известные на рынке профессионалы, такие компании, как «АМДтехнологии», «Свободные Технологии Инжиниринг», «Т1 Интеграция».

Базовая модель эксплуатации – все делаем сами. Но рассматриваем и другие варианты. Ведем переговоры с компаниями, которые могли бы взять эксплуатацию объекта на себя. Если получится договориться на хороших условиях, будем такие компании привлекать. Но при этом планируем, что ключевые сотрудники – главный механик, главный энергетик, технический директор и т.п. – будут наши, а остальной персонал – эксплуатирующей организации. Склоняемся к такому, гибридному варианту.

– Сегодня деньги дорогие. Сроки возврата инвестиций выросли. Вас это не смущает?

– Знаю, что цодостроители привыкли к срокам возврата инвестиций семь-восемь лет. Мы же как девелоперы всегда работали на рынке, где этот срок составляет около 10 лет. Для нас это нормально.

Пока в этом проекте кредитное плечо у нас маленькое. Большие затраты пойдут через год, когда начнем закупать дорогостоящее оборудование. Надеюсь, к тому моменту ставка снизится.

– Насколько для вас важна энергоэффективность?

– Конечно, этот вопрос учитывался при выборе решений. Например, чиллеры будут поддерживать функцию естественного охлаждения (фрикулинга). Проектное значение PUE – 1,37. Реальное будет, конечно, чуть больше, но все равно, надеемся, что не выше среднемировых значений (1,56).

– Вы упомянули, что проект рассчитан на среднюю мощность стойки 5 кВт. Однако сейчас, с ростом интереса к системам на базе искусственного интеллекта, все чаще запрашивают более мощные стойки. Предусмотрены ли они проектом?

– На самом деле для подобных проектов правильнее оперировать понятием энергетической плотности на квадратный метр машинного зала. Сейчас мы рассматриваем стандартные 600-мм стойки, и именно такая геометрия при максимально плотном размещении дает мощность 5 кВт на стойку. Но использование водяного чиллерного охлаждения и свобода в выборе систем внутризального кондиционирования в сочетании с другими, более современными размерами стоек позволяет нам гибко конфигурировать тепловую мощность стойки в зависимости от потребностей заказчиков. За счет зонирования, конечно, можно будет устанавливать и более мощные стойки, например, 12–15 кВт.

Кроме того, на каждом этаже запроектированы зоны для мегаплотных стоек, для которых предполагается использовать системы прямого жидкостного охлаждения. Вплоть до 50 кВт и выше. Так что к всплеску спроса на системы для искусственного интеллекта мы тоже готовимся.

– Вы ориентируетесь на наивысший уровень надежности – Tier IV. С чем связан такой выбор? Почему не Tier III, как большинство российских коммерческих ЦОДов?

– Не скрою, в нашей команде были жаркие споры: Tier III или Tier IV. В пользу Tier IV нас склонили, пожалуй, два основных фактора. Во-первых, в отличие от ЦОДов Tier III объекты Tier IV являются более отказоустойчивыми. В наше неспокойное время – а вероятность ЧП возросла – секционирование инженерных систем и другие меры, которые предусмотрены Tier IV, становятся все более значимыми. Для заказчиков это важно.

Во-вторых, расчеты показали, что разница в стоимости проектов Tier III и Tier IV невелика, несколько процентов от общих затрат. Получается, что относительно небольшими дополнительными затратами мы существенно снижаем риски, получаем более высокую надежность, отказоустойчивость.

Кстати, именно поэтому мы выбрали подключение по второй категории надежности электроснабжения. Хотя были те, кто советовал сэкономить и подключиться по третьей. Но мы выбрали надежность.

Она важна еще и потому, что мы в целом позиционируем Alcon DC Nord как премиальный объект. У здания будут красивые фасад и входная группа, качественная отделка помещений. Кроме того, окружающая жилая застройка района сделала необходимой минимизацию шумового и визуального загрязнения от ЦОДа, что было достигнуто за счет использования современных архитектурных решений и глубокой интеграции элементов инженерной инфраструктуры в строительные конструкции. Такой подход позволяет нам заявить о своем проекте как о новом взгляде на архитектурный и функциональный облик технопарков. Считаю, что хороший ЦОД должен быть красив и снаружи, и внутри, и конечно, инженерные решения должны быть наивысшего уровня. А это Tier IV.

– Что вас подвигло заняться цодостроительством? Насколько для вас важно это направление?

– Мы увидели и оценили долгосрочные перспективы этого рынка. Цифровизация экономики, госуправления, общественной жизни и внедрение в них искусственного интеллекта, взрывное развитие нейросетей, беспилотный транспорт – все это требует быстрого развития цифровой инфраструктуры. И рынок ЦОДов устойчиво растет.

Alcon DC Nord – наш пилотный проект в области цодостроения, который будет иметь продолжение. В середине 2025 г. посмотрим, как идет стройка, каков отклик рынка, как реагируют потенциальные заказчики. После этого скорректируем наши ожидания, финансовую модель и будем принимать решения по следующим проектам.

Надежность систем ИБП. Что выбирают ЦОДы

Александр Барсков

Как показало исследование, проведенное совместно «Парус электро» и iKS-Consulting, в российских ЦОДах для ИБП наиболее популярна схема резервирования N + 1, а возможности и вариативность схем резервирования существенно повышаются при использовании модульных ИБП.

Непрерывность функционирования критичных ИТ-сервисов в ЦОДах во многом определяется качественным бесперебойным электропитанием соответствующего ИТ-оборудования. В свою очередь, для надежного, отказоустойчивого функционирования источников бесперебойного питания (ИБП) в ЦОДах прибегают к различным вариантам их резервирования. Чтобы выяснить предпочтения российских компаний при выборе схем (топологий) резервирования, отечественный производитель ИБП компания «Парус электро» и аналитическое агентство iKS-Consulting провели совместное исследование, в ходе которого также были изучены особенности (преимущества) обеспечения отказоустойчивости при использовании модульных ИБП. Результаты исследования были представлены на совместной конференции в апреле 2024 г.

В рамках исследования было опрошено более 40 специалистов предприятий, имеющих собственные ЦОДы и серверные. На вопросы отвечали технические директора, руководители технических подразделений и ведущие эксперты, деятельность которых связана с построением и эксплуатацией систем бесперебойного питания.

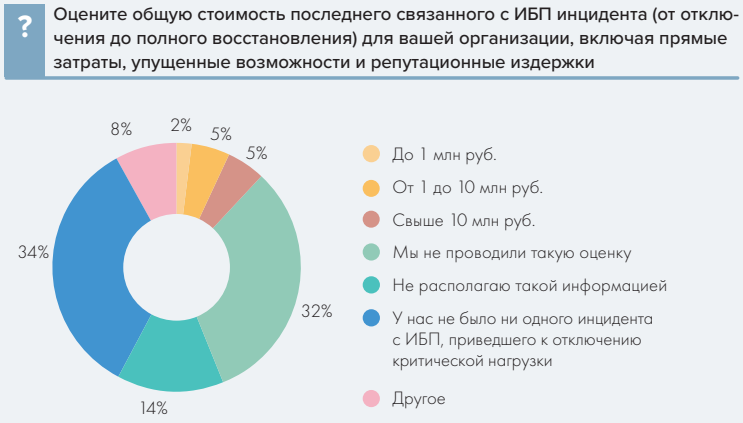
Большинство участников исследования (примерно 80%) эксплуатируют комплексы ИБП общей мощностью 100 кВт и выше. На объектах 15% респондентов установлены системы бесперебойного питания общей мощностью более 10 МВт.

Подавляющее большинство респондентов эксплуатируют статические ИБП (рис. 1). Как показывает анализ данных исследования, примерно половина используют и моноблочные, и модульные устройства. Только 10% опрошенных применяют динамические ИБП, и половина из них также имеют в своем хозяйстве модульные статические аппараты. Очевидно, что статические ИБП доминируют в российских ЦОДах, причем доля модульных устройств превышает долю моноблочных.

По данным Uptime Institute, проблемы с электроснабжением – главная причина отказов ЦОДов, и доля соответствующих инцидентов растет: в 2020 г. она составила 37%, в 2021 г. – 43%, в 2022 г. – 44%. Причем поломка ИБП – основная причина инцидентов, связанных с электроснабжением. На нее, согласно исследованию Uptime Institute Data Center Resiliency Survey, в 2023 г. пришлось 40% таких инцидентов.

Стоимость той или иной аварии – обычно болезненная тема для респондентов, и на такие вопросы они отвечают крайне неохотно. Тем не менее в ходе опроса, проведенного «Парус электро» и iKS-Consulting, ряд специалистов оценили общую стоимость последнего связанного с ИБП инцидента (от отключения до полного вос-

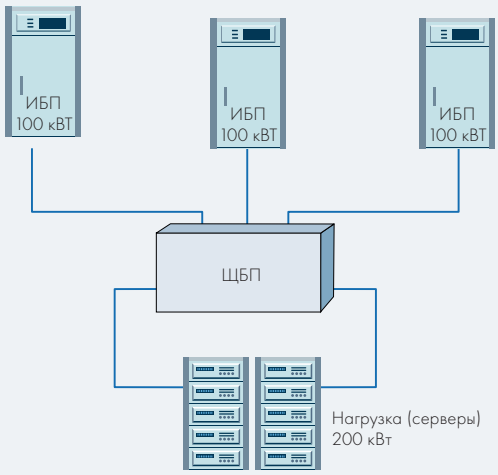
▲ Рис. 1. Состав системы бесперебойного питания в компаниях – участниках исследования



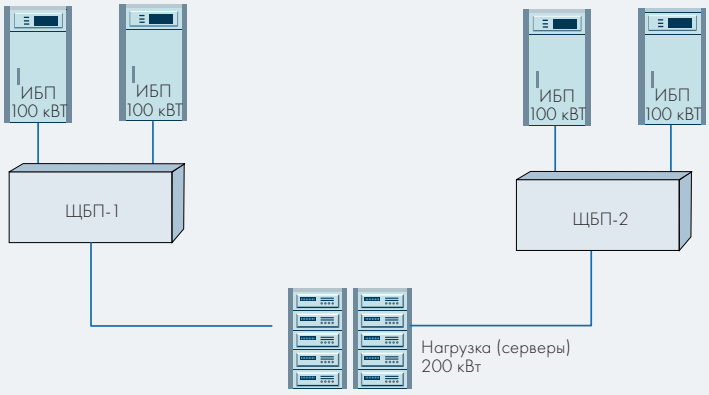
▲ Рис. 2. Стоимость инцидента, связанного с ИБП

▲ Рис. 3. Схемы резервирования ИБП, используемые в ЦОДах

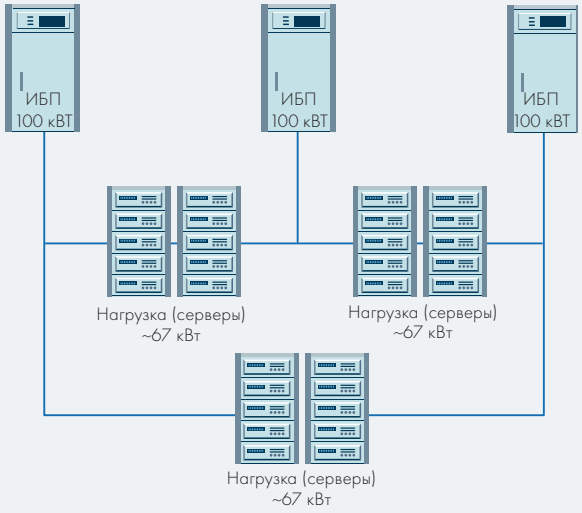
Источник: Исследование «Надежность систем ИБП», «Парус электро», iKS-Consulting, 2024 г.



▲ **Рис. 4. Пример схемы резервирования N+1**



▲ **Рис. 5. Пример схемы резервирования 2N**



▲ **Рис. 6. Пример схемы резервирования 3N/2**

Источник: Исследование «Надежность систем ИБП», «Парус электро», iKS-Consulting, 2024 г.

становления) для своей организации (рис. 2). Только в трети компаний ответили, что у них не было ни одного инцидента с ИБП, приведшего к отключению критической нагрузки.

Схемы резервирования

Резервирование предполагает определенную избыточность компонентов объекта, благодаря которой при отказе одного или даже нескольких компонентов можно избежать прерывания работы объекта в целом. Базовую модель резервирования описывают формулой N + R, где N (от англ. normal) – число элементов, необходимых для нормальной работы, а R (от англ. redundant) – число избыточных компонентов. Это резервирование на уровне компонентов, в нашем случае – на уровне отдельных ИБП (модулей ИБП).

Наиболее известна схема резервирования на уровне компонентов N + 1. Она же, как показало исследование, наиболее популярна в российских ЦОДах – ее используют более 60% респондентов (рис. 3).

В качестве примера рассмотрим ЦОД с ИТ-нагрузкой 200 кВт. Для ее обслуживания можно установить, скажем, два ИБП по 100 кВт (N + 0). Чтобы организовать резервирование по схеме N + 1, необходимо установить в параллель еще один такой ИБП (рис. 4).

На практике встречаются варианты N + 2 или даже с большим числом элементов R. Одним из важных преимуществ схемы N + 2, которую использует примерно каждый восьмой ЦОД в России, является то, что во время отказа или технического отключения одного из ИБП в системе сохранится избыточность (N + 1).

Чтобы снизить общую мощность резервируемой системы, можно пойти по пути уменьшения мощности отдельных ИБП: например, для 200-кВт нагрузки выбрать четыре ИБП по 50 кВт, а еще один такой же источник установить в параллель. Если развивать этот подход дальше, то можно рассмотреть вариант с 10 ИБП по 20 кВт плюс один резервный. В настоящее время привлекательность такого подхода повышается в связи с тем, что источники меньшей мощности зачастую более доступны, поскольку являются, например, частью складской программы поставщика. Однако при увеличении числа компонентов, включая кабельные соединения и пр., надежность может снижаться. Проектировщики нередко следуют эмпирическому правилу добавления одного резервного компонента на каждые четыре (максимум пять) необходимых.

К основным преимуществам схем N + R следует отнести относительную простоту как самой системы, ее масштабирования и эксплуа-

тации, так и управления нагрузкой. Главный недостаток – более низкая надежность по сравнению с системами 2N (которые будут описаны ниже). Так, в системе, показанной на рис. 4, присутствует единая точка отказа в виде распределительного щита бесперебойного питания (ЩБП).

В схемах 2N резервируется система целиком, резервируемые компоненты полностью разделены (для достижения отказоустойчивости их рекомендуют размещать в разных помещениях). Поскольку системы ИБП полностью отделены друг от друга, они могут строиться на аппаратах разных моделей и даже разной мощности, хотя в последнем случае управлять нагрузкой будет сложнее. В России схему 2N используют примерно 10% компаний (см. рис. 3).

В нашем примере (рис. 5) – две независимые системы ИБП, мощности каждой достаточно для питания нагрузки. В штатном режиме каждая система ИБП обеспечивает половину необходимой мощности для нагрузки, имеющей два блока питания, каждый из которых подключен к отдельному лучу. (При наличии в серверах только одного блока питания рекомендуют устанавливать в стойку АВР.) В случае выхода из строя одной системы ИБП нагрузка автоматически переходит полностью на питание от другой.

Более высокий уровень резервирования может быть достигнут, если в каждой из систем организовать резервирование по схеме N + 1. В нашем примере потребуется установить в каждой системе три ИБП по 100 кВт. Это вариант 2(N + 1). Даже если одна из систем ИБП полностью выйдет из строя, необходимая мощность будет обеспечена, да еще с резервированием. Такой, наиболее дорогостоящий из рассмотренных, вариант используется в основном в финансовых учреждениях или в случаях, когда необходимо защитить критическую нагрузку.

Табл. 1. Загрузка ИБП при реализации различных схем резервирования ▼

Схема резервирования	Резервная мощность, кВт	Число ИБП (модулей) по 100 кВт	Максимальная загрузка модуля в штатном режиме при полной загрузке системы, %
N + 0	0	2	100
N + 1	100	3	67
N + N (2N)	200	4	50
2(N + 1)	400	6	33
3N/2	100	3	67

Источник: Исследование «Надежность систем ИБП», «Парус электро», iKS-Consulting, 2024 г.

При выборе схемы резервирования на первом месте стоит обеспечение непрерывного функционирования нагрузки. Но, конечно, важна и стоимость решения. Для ее оценки можно опираться на показатель загрузки отдельных ИБП (модулей), который оказывает прямое влияние на капитальные и эксплуатационные расходы по двум причинам:

- чем выше загрузка ИБП, тем, как правило, выше их КПД (хотя во многих устройствах последнего поколения уровень КПД примерно одинаков при загрузке 25–30% и выше);
- чем ниже загрузка, тем больше ИБП требуется, а значит, тем выше капитальные затраты.

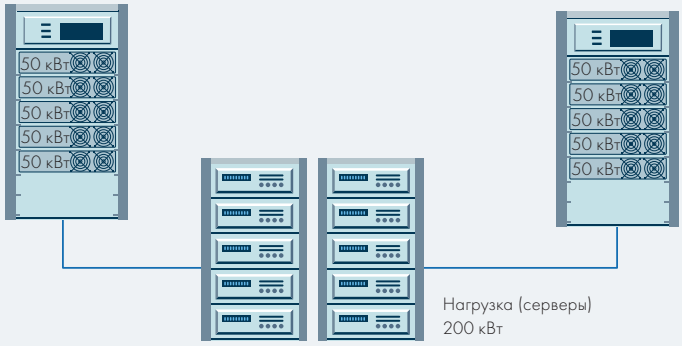
При повышении уровня резервирования увеличивается число ИБП и, соответственно, снижается уровень их загрузки (табл. 1). Из представленных в табл. 1 решений система 2(N + 1) обеспечивает максимальную избыточность, но наименьшую загрузку ИБП – всего 33%. В нашем примере для реализации такой системы с нагрузкой 200 кВт требуется установить ИБП общей мощностью 600 кВт – в три раза больше мощности нагрузки.

В последние годы все больше внимания привлекают так называемые дробные, или распределенные, схемы резервирования, которые обеспечивают две независимые линии электропитания нагрузки, как в вариантах 2N и 2(N + 1), но при этом позволяют повысить загрузку отдельных ИБП и снизить расходы. Такие схемы предполагают сегментирование ИТ-нагрузки. Их обозначают (XN/Y), где X – число установленных элементов (ИБП) в системе, а Y — число групп ИТ-нагрузки, подключенных к каждому из элементов.

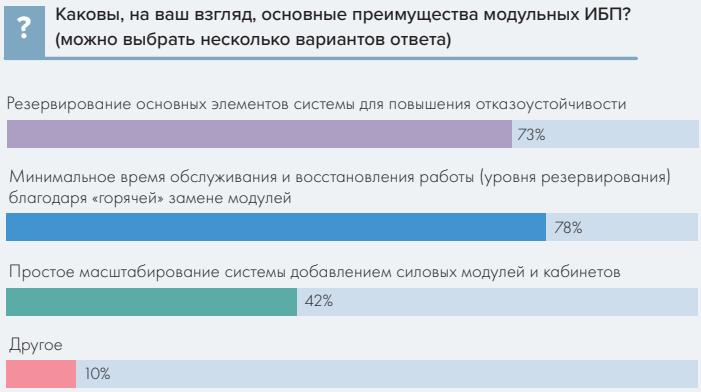
Пример резервирования 3N/2 для нагрузки суммарной мощностью 200 кВт приведен на рис. 6: каждая группа ИТ-нагрузки получает электропитание от двух независимых линий (ИБП), однако общая мощность системы ИБП меньше, чем в варианте 2N. При выборе схемы 3N/2 затраты на ИБП сопоставимы с затратами на схему N + 1, однако уровень отказоустойчивости выше.

Можно увеличивать дробность, скажем, делать системы 4N/3, 5N/4 и т.д., что будет повышать загрузку отдельных элементов. Но надо понимать, что при этом будет усложняться система кабельной разводки, соответственно, увеличиваться объем необходимых материалов и работ. Более того, управление нагрузкой в таких системах также будет усложняться, что повысит риск ошибок, связанных с человеческим фактором.

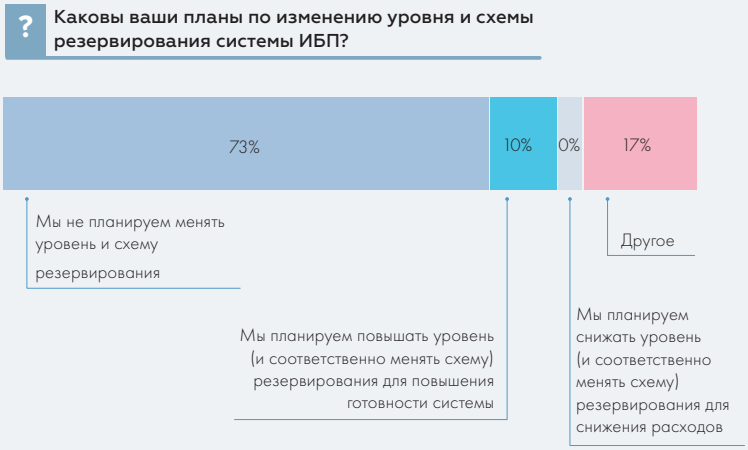
В результате система с большим числом компонентов может оказаться менее надежной, чем базовая система N + 1, именно потому, что име-



▲ Рис. 7. Пример реализации резервирования 2(N + 1) на базе модульного ИБП



▲ Рис. 8. Основные преимущества модульных ИБП



▲ Рис. 9. Планы по изменению уровня и схемы резервирования системы ИБП

Источник: Исследование «Надежность систем ИБП», «Парус электро», iKS-Consulting, 2024 г.

ет много компонентов, которые могут выйти из строя, и несколько точек балансировки нагрузки. По мнению ряда экспертов, 6N/5 – предельная дробность для систем резервирования. Более высокие уровни очень сложны в реализации и теряют свои экономические преимущества. Хотя в российских ЦОДах есть примеры успешного использования даже схемы 8N/7.

Особенности резервирования при использовании модульных ИБП

Возможности резервирования электропитания существенно повышаются при использовании модульных ИБП. Если в классических моноблочных ИБП выходная мощность обеспечивается одним силовым блоком, то модульный состоит из функционально независимых силовых модулей, которые можно заменять в «горячем» режиме, т.е. без отключения ИБП и нагрузки. Каждый такой модуль оснащается инвертором, выпрямителем, зарядным устройством и представляет собой полноценную силовую часть ИБП. Мощность силовых модулей разных моделей ИБП различна, например, 20, 50 или 100 кВт. Помимо силовых модулей в современных модульных ИБП может быть установлено несколько модулей управления, которые также заменяются в «горячем» режиме. Функция «горячей» замены может распространяться и на модуль байпаса.

Применение модульных ИБП дает ряд существенных преимуществ при реализации резервирования. Так, в нашем примере для поддержки ИТ-нагрузки 200 кВт систему бесперебойного питания с резервированием по схеме N + 1 можно построить на основе одного ИБП с силовыми модулями 50 кВт путем установки в него пяти таких модулей. При этом установленная мощность составит 250 кВт, а загрузка модулей – 80%. Дальнейшее масштабирование (или повышение уровня резервирования до схемы N + 2) возможно путем простого добавления модулей в установленное шасси, тогда как при использовании моноблоков потребуется установка еще одного ИБП – соответственно, дополнительное место, расходы на его оборудование, каблирование и пр. Единственный серьезный недостаток работы с одним модульным аппаратом – невозможность разнести его по разным помещениям.

Этот недостаток устраняется установкой нескольких модульных ИБП в разных помещениях. Для нашего примера схему 2(N + 1) можно реализовать, установив два таких ИБП с пятью 50-кВт модулями в каждом (рис. 7).

Как показал проведенный опрос, из тех компаний, которые применяют модульные ИБП, примерно три четверти задействуют преимущества

Схема резервирования	Уровень надежности	CAPEX	OPEX	Сложность	Занимаемая площадь
N	2	10	8	10	10
N + 1	4	8	9	9	9
N + 2	5	6	8	9	8
3N/2	5	5	6	2	5
2N	6	3	4	5	4
2(N + 1)	9	2	2	4	2

Оценка по 10-балльной шкале, где 10 – наилучший показатель, а 1 – наихудший

◀ Табл. 2. Экспертная оценка параметров различных схем резервирования

Источник: Исследование «Надежность систем ИБП», «Парус электро», iKS-Consulting, 2024 г.

резервирования модулей. Причем примерно половина из них используют только резервирование модулей в самом ИБП, а еще столько же – и резервирование модулей в ИБП, и резервирование ИБП. В целом установка резервных модулей не только обеспечивает некоторую избыточность самого ИБП, повышая его надежность, но и образует некую матричную структуру в связке с другими ИБП параллельной системы, которая автоматически перераспределяет общую нагрузку среди работающих модулей.

Важное преимущество модульных ИБП – минимизация времени обслуживания и восстановления работы (уровня резервирования) благодаря «горячей» замене модулей. Это преимущество отметили 78% опрошенных (рис. 8). Запасные модули можно предусмотреть в ЗИПе на складе недалеко от объекта или на самой площадке, а их замену в случае необходимости могут выполнить сотрудники самой компании. Это позволяет существенно снизить показатель MTTR, а значит, максимально оперативно восстановить работу ИБП или вернуть устройство к заложенному в проект уровню резервирования (избыточности).

Примерно 40% респондентов отметили такое преимущество модульных ИБП, как возможность простого и быстрого (при наличии на площадке) добавления силовых модулей. Это дает возможность оперативно наращивать мощность системы бесперебойного питания по мере необходимости, что, в свою очередь, означает постепенность инвестиций и сохранение высокого уровня загрузки имеющихся ресурсов (модулей).

Данные опроса показывают, что доля модульных ИБП будет увеличиваться. Так, 23% респондентов указали на то, что используют и модульные, и моноблочные ИБП и будут наращивать долю модульных. А примерно 5% планируют отказаться от моноблочных устройств в пользу модульных.

Критерии выбора

При выборе схемы резервирования для компании на первом месте стоит, конечно, надежность – гарантия того, что ни при каких обстоятельствах не произойдет отключения критической нагрузки. Но, как показал проведенный опрос, учитываются и другие показатели: расходы (CAPEX и OPEX), сложность системы и занимаемая ею площадь.

Так, усложнение системы непосредственно связано со сложностью обслуживания, а значит, с повышением рисков отказа, обусловленных человеческим фактором. Этот фактор влияет и на то, что большинство компаний выбирают схему N + 1, которая наименее сложна в реализации и обслуживании. Что касается минимизации занимаемой площади, то этот показатель наиболее важен для коммерческих ЦОДов, которые зарабатывают на продаже площадей (стойко-мест).

Экспертная оценка основных схем резервирования по рассмотренным критериям приведена в табл. 2. Как уже отмечалось, наивысший уровень надежности обеспечивает схема 2(N + 1), но она же требует наибольших расходов и наибольшей площади. Дробный вариант 3N/2 выглядит сбалансированным по всем основным показателям, но характеризуется наибольшей сложностью.

Как показало исследование, в выборе схем резервирования компании крайне консервативны. Подавляющее большинство (73%) не планируют менять ни уровень, ни схему резервирования (рис. 9). Никто из респондентов не собирается снижать уровень резервирования ради снижения расходов. И примерно 10% планируют повышать уровень (и соответственно менять схему) резервирования для повышения готовности системы. Последнее обстоятельство иллюстрирует значимость надежного функционирования системы бесперебойного питания. ИКС

Итальянское качество при стабильных поставках

Один из мировых лидеров рынка холодильного оборудования предлагает современные решения для российского рынка. О компании «Кливет» рассказывает председатель совета директоров российского подразделения Вероника Сильвестрова.

– Вероника Вячеславовна, расскажите об истории создания компании, о том, где находятся производственные мощности, когда она вышла на российский рынок и в каких сегментах присутствует.

– Компания Clivet S.p.A создана в 1989 г. в городе Фельтре, расположенном в Доломитовых Альпах на севере Италии. Принципы компании отражены в названии торговой марки: CLIVET расшифровывается как Clima Innovazione Via Energetico efficienza Tecnologia, что в переводе на русский означает «Инновации в климате через энергоэффективные технологии». Компания Clivet начала работу с выпуска чиллеров и тепловых насосов, затем перешла к другим видам холодильного оборудования.

В России первые чиллеры Clivet появились около 30 лет назад. В 2007 г. было решено открыть здесь дочернюю компанию. Генеральным директором представительства стал известный итальянский бизнесмен Витторио Торрембини. Общая численность сотрудников на этом этапе была всего 15 человек. Несмотря на глобальный экономический кризис 2008 г., уже за первые три года работы представительства команде удалось добиться значительных результатов и реализовать целый ряд знаковых проектов.

В настоящий момент наша команда в России насчитывает более 50 человек, большая часть сотрудников – инженеры по сервису и технической поддержке.

В 2016 г. Midea Group, китайский гигант рынка бытовой техники, электроприборов и кондиционирования воздуха, приобрел акции компании Clivet. Сделка имела синергетический эффект для обеих компаний. Были сделаны значительные инвестиции в производство Clivet в Италии, построены новые цеха и лаборатории. У российского подразделения появились дополнительные возможности благодаря поставкам новых групп оборудования, в том числе чиллеров с центробежными компрессорами. Поставки стали осуществляться не только с заводов в Италии, но и с заводов Midea в Китае.

В настоящее время Clivet – один из мировых лидеров климатического оборудования, экспортирующий продукцию в 90 стран мира. Компания имеет собственные подразделения в России, Юго-Восточной Европе, Германии, Франции, Великобритании, Индии, Китае и на Ближнем Востоке.

– Как в компании организованы проектные и изыскательские работы?

– У Clivet крупные R&D-дивизионы в Италии и Китае, определяющие направления развития холодильного оборудования компании. Российское подразделение компании также участвует в формировании продуктовой линейки с учетом локальной специфики. Досконально зная возможности оборудования, российское подразделение помогает клиентам выбрать оптимальный для их запросов вариант.

В 2022 г. открылся новый Инновационный центр Clivet в г. Фельтре, основная задача которого – непрерывное повышение качества и скорости разработки оборудования. Благодаря дополнительным испытательным камерам и новым тестам Clivet может проводить больше функциональных, эксплуатационных, акустических, вибрационных и стрессовых испытаний при различных параметрах температуры воздуха. Наши клиенты могут увидеть запуск и работу своих машин, присутствуя на испытаниях непосредственно в Италии или удаленно.

– Как компания работает с российскими дата-центрами?

– Работа по направлению дата-центров ведется не только на российском рынке, это один из фокусов внимания компании во всех странах присутствия. Международная команда инженеров и менеджеров по развитию продукта развивает данное направление на протяжении нескольких лет, дорабатывая продуктовую линейку в соответствии со спецификой дата-центров. Говоря об этом направлении в России, мы рады отметить, что в текущем году мы поставили оборудование для нескольких российских дата-центров. Задействован Инновационный центр в Италии: в этом году мы в присутствии специалистов нашего партнера – центра компетенций ООО «АМДтехнологии» – и наших заказчиков проводили там тестирование чиллера 1,2 МВт из поставки для российского ЦОДа суммарной мощностью около 6 МВт.

– В чем конкурентные преимущества компании на российском рынке дата-центров? Какие решения наиболее востребованы?

– Прежде всего это хорошая репутация, европейские требования к качеству всей линейки оборудования, использование современных технологий и стабильность поставок. 30 лет компания входит в топ производителей, поставляющих чиллеры на российские объекты. При этом мы поставляем только те чиллеры, которые производим сами: воздушные, бесконденсаторные, водяные, с винтовыми, спиральными и центробежными компрессорами. В разработке оборудования для ЦОДов участвуют наши международные команды, взаимно обогащая друг друга экспертизой работы на рынках разных стран.

В числе других конкурентных преимуществ – широта линейки, в которой найдутся решения для самых специфичных требований. Также стоит отметить стабильность и надежность: оборудование работает без сбоев вне зависимости от климатических условий и сложности нагрузок.

Отличительная особенность – внимание к энергосбережению, оптимизирующее эксплуатационные расходы. Кроме того, компания уделяет повышенное внимание вопросам экологии, например, переходит на хладагенты с малым воздействием на окружающую среду. На заводах не только собираются и полностью тестируются чиллеры, но и выпускается широкий ряд комплектующих для них, что позволяет гарантировать качество. Комплектующие и готовая продукция хранятся на полностью автоматизированных складах, что сокращает сроки поставки оборудования.

Наибольшим спросом в России пользуются чиллеры мощностью около 1 МВт. В то же время в портфеле компании есть чиллеры с воздушным охлаждением конденсатора до 1,7 МВт и водяным охлаждением конденсатора мощностью до 6 МВт.

– Какая используется модель продаж? Как организована поддержка продукции Clivet в России? Проводится ли обучение российских специалистов, дистрибьюторов и заказчиков?

– Основной принцип нашей работы – вовлеченность в проект наших заказчиков. Мы поставляем не только само оборудование, но и нашу поддержку, как на этапе выбора концепции холодоснабжения, так и на этапе эксплуатации оборудования.

В Москве открыт филиал итальянского CLIVET University для обучения технических специалистов наших партнеров, начиная от проектировщиков и заканчивая инженерами службы эксплуатации. На этой площадке также размещен демонстрационный зал оборудования с постоянно обновляемой экспозицией.

Регулярно проводятся обучение и тестирование работников сервисных центров, рабочее обсуждение возникающих у них проблем. Формат разный: и онлайн, и офлайн, если требуется работа с оборудованием. Важно, что специалисты получают не только теоретические знания, но и опыт практической работы с продуктами компании.

В текущем году демонстрационные залы будут открыты в Санкт-Петербурге и в нашем представительстве в Ростове. В следующем году представительства появятся в Татарстане и Сибири.

– Есть ли публичные примеры внедрения решений Clivet в российских дата-центрах?

– В российских дата-центрах много холодильного оборудования Clivet, поставляемого под другими брендами. Но учет такого оборудования мы не ведем. Есть и внедрения под брендом Clivet, но не публичные.

– Каковы финансовые итоги прошлого года? Каковы ближайшие и долгосрочные планы развития в России? Какие еще продукты планируется вывести на российский рынок?

– На июньской конференции Midea MBT, которая проходила в Чунцине, российское подразделение подвело итоги по каждому направлению. План прошлого года выполнен в полном объеме. Теперь перед нами стоят новые задачи. В частности, по холодильным машинам намечено увеличить объем поставок в два раза за три года. Большим подспорьем для нас будет новая линейка продуктов для ЦОДов, которую мы анонсируем уже этой осенью.

Дмитрий Шпанько, директор по развитию, Powercom

Когда ЦОДы становятся большими

Разработав мегаваттные ИБП, дополнив свой портфель системами кондиционирования, PDU и стойками, компания Powercom значительно усилила свои позиции на рынке цодостроения.

– Powercom многие годы лидирует на российском рынке ИБП. Как компания чувствует себя на рынке систем электропитания для ЦОДов, где востребованы мощные трехфазные аппараты?

– Направление мощных трехфазных ИБП мы начали активно развивать лет шесть-семь назад, за прошедшее время серьезно нарастили компетенции и сейчас чувствуем себя на этом рынке уверенно. Постепенно в рамках направления мы стали фокусироваться на продуктах для ИТ-комплексов, для центров обработки данных. А последние годы работа на рынке ЦОДов сделалась для нас приоритетной.

Хотя ИБП в принципе достаточно универсальный продукт, со временем мы поняли, что в ЦОДах есть своя специфика, и устройства для таких объектов надо разрабатывать специально. В текущем году выпустили линейку мощных ИБП именно для ЦОДов, что дало нам дополнительную уверенность и преимущества на рынке. Теперь мы предлагаем модульные ИБП с мощностью единичного устройства до 1,2 МВт (модули по 100 кВт). Восемь ИБП можно объединить в параллельную систему, что позволяет получить комплекс мощностью до 9,6 МВт, а в случае резервирования по схеме N + 1 – 8,4 МВт. Этого вполне достаточно даже для мегаЦОДов. Именно благодаря тому, что компания выпустила более мощные ИБП модульного типа, мы смогли принять участие в проектах, для которых раньше нам просто нечего было предложить. И проекты с использованием упомянутых ИБП уже реализуются.

– Какие тенденции можете отметить на рынке цодостроения в целом? Как Powercom соответствует этим тенденциям?

– Первой тенденции мы уже частично коснулись. Это увеличение масштаба проектов. Если говорить о коммерческих ЦОДах, то в Москве, например, емкость практически всех строящихся ЦОДов исчисляется тысячами стоек. Растут масштабы ЦОДов в регионах. Это же относится и к корпоративным объектам. Поэтому производителям, у которых в портфеле нет мощных, мегаваттных ИБП, сегодня нечего предложить для таких проектов. Мы своевременно уловили эту тенденцию и успели подготовить соответствующие решения.

Растет не только число стоек в ЦОДах, но и плотность мощности стоек. Этот тренд касается и оборудования ИБП. Заказчикам требуется размещать ИБП все большей мощности на малой площади. Поэтому уже сегодня активно применяются силовые модули до 100 кВт. Думаю, мощность одного модуля будет увеличиваться и дальше. Наши решения позволяют разместить ИБП на 1,2 МВт в одной стойке (правда, нестандартной). Получается около 600 кВт на 1 кв. м – это высокий показатель.

Следующая тенденция – повышение гибкости, вариативности технических решений. Приведу два примера. Первый – универсальность подключения кабельных вводов ИБП. В предыдущем поколении наших устройств ввод кабеля был сверху. Поэтому нам сложно было предлагать их для проектов с фальшполами, когда кабели подводятся снизу. Новые модели универсальны: при заказе можно выбирать, какой ввод делать – сверху или снизу, и это никак не влияет ни на стоимость ИБП, ни на сроки производства.

Второй пример – поддержка различных типов АКБ. Сегодня почти во всех крупных проектах заказчик просчитывает два варианта: на свинцово-кислотных и литий-ионных батареях. Расчет усложняется, если делать его для разных моделей ИБП. Более того, бывают случаи, когда заказчик предусматривает универсальное батарейное помещение, а ИБП выбирает уже на этапе закупок. Все наши модульные ИБП готовы работать с обоими типами АКБ, и спецификация ИБП остается неизменной. Это дает заказчику определенную гибкость в выборе АКБ.

Отмечу еще одну важную тенденцию – повышенное внимание к показателю КПД, особенно у крупных компаний и коммерческих ЦОДов. Для ряда российских компаний с большими собственными ЦОДами важна «зеленая» повестка. Некоторые полностью или частично отказываются от классических кондиционеров и чиллерных систем. Недавно мы реализовали проект создания крупного ЦОДа (3 МВт) на фрикулинге, так там при выборе ИБП значение КПД было чуть ли не решающим критерием: в помещениях для ИБП из-за отсутствия кондиционирования температура повышается, поэтому важен каждый процент КПД, влияющий на тепловыделение. Наше оборудова-

ние успешно работает уже несколько месяцев в самую жаркую погоду.

– Какой уровень КПД сейчас устраивает таких заказчиков?

– Показатели наших ИБП заказчиков вполне устраивают. Это 96% в онлайн-режиме (с двойным преобразованием) в широком диапазоне нагрузки. В экорежиме КПД еще на пару процентов выше. Но лишь немногие ЦОДы используют такой режим, хотя примеры есть.

Кроме того, наши ИБП штатно работают при температуре 40°C. Это при полной нагрузке. Чаще ИБП функционируют при частичной нагрузке, тогда могут работать при 45–50°C.

– Как вы доказываете, что при эксплуатации объекта КПД будет именно 96%? Где гарантия, что он не упадет, скажем, до 90% или еще ниже?

– Во-первых, у Powercom многолетняя хорошая репутация, и мы ей очень дорожим. Во-вторых, характеристики ИБП мы готовы подтвердить протоколами тестирования на заводе – его проходит каждый мощный аппарат. И в-третьих, мы готовы на любые проверки. Такие проверки для многих крупных заказчиков становятся уже обязательным условием включения производителя в вендор-лист. По просьбе заказчиков испытания неоднократно проводились независимыми лабораториями в России, и в случае с нашими ИБП всегда успешно.

– Говоря о тенденциях, наверное, надо сказать и о росте требований к надежности. А здесь важен не только продукт, но и сервис.

– Конечно, для любого заказчика, а уж тем более для ЦОДов, надежность важна. А для ее обеспечения необходимо учитывать много моментов: и качество самого продукта, и архитектуру системы, и конечно, сервисное обслуживание.

Сегодня все больше заказчиков из отрасли ЦОДов запрашивают модульные ИБП, что позволяет повысить отказоустойчивость систем бесперебойного питания. Использование модульной архитектуры вкупе с обученной службой эксплуатации дает заказчику возможность в случае инцидента оперативно заменить модуль и восстановить первоначальное состояние системы. С этой целью все больше компаний запрашивают расширенный ЗИП для размещения на площадке. Есть случаи, когда заказчик уже в начале проекта закупает запасные силовые модули, вентиляторы и другие элементы, чтобы минимизировать время реакции в проблемных ситуациях.

Время реакции нашей сервисной службы, конечно, зависит от территориального расположения объекта. В крупных городах, таких как Москва, Санкт-Петербург, Новосибирск, Владивосток, мы сами можем обеспечить четырехчасовое время реакции. Но если объект удален, то рекомендуем модульную архитектуру, расширенный ЗИП на площадке и обучение инженеров заказчика.

Для небольших удаленных объектов (серверных комнат, edge-ЦОДов) предлагаем новую услугу – предзапуск ИБП. Мы делаем предварительные настройки ИБП для конкретного проекта и потом отгружаем клиенту – ему достаточно только подключить аппарат к электросети и к нагрузке. Это особенно востребовано в ситуациях, когда стоимость выезда квалифицированных инженеров превышает стоимость самих ИБП. Такое часто случается при установке аппаратов мощностью 10–20 кВт на удаленных объектах, куда добираться сложно, долго и дорого.

– Недавно Powercom начала предлагать полные (комплексные) решения для инженерной инфраструктуры ЦОДов. Усилило ли это позиции компании на рынке цодостроения?

– Да, мы усилили свои позиции. Наличие комплексного решения, включающего системы кондиционирования, стойки, блоки распределения питания (PDU), существенно расширило круг наших партнеров и заказчиков. Отношение к компании меняется, повышается узнаваемость бренда. У нас уже есть успешные проекты, для которых помимо традиционных для нас ИБП мы поставляем и другие продукты в рамках комплексного решения.

– В России Powercom работает давно. А присутствует ли компания в соседних странах? Как оцениваете перспективы соответствующих рынков?

– Уже очень давно присутствуем в Беларуси. Есть дистрибьютор, много партнеров, бизнес хорошо развивается.

В прошлом году приняли решение серьезно активизировать работу в Центральной Азии. Речь идет в первую очередь о Казахстане, Узбекистане и Киргизии. Экономика там растет, идет активная цифровизация государственного и банковского секторов. Отрасль ЦОДов в этих странах пока невелика, но быстро развивается. Развиваем нашу деятельность и мы. Уже есть контракты с местными дистрибьюторами, есть авторизованные партнеры. В Казахстане и Киргизии открыли сервисные центры, скоро откроем в Узбекистане. Так что рассчитываем на увеличение присутствия оборудования Powercom как в российских ЦОДах, так и в дата-центрах стран Центральной Азии.

Экономика проектов выходит на первое место

Как меняются подходы к созданию ЦОДов: требования к надежности, мощности стоек, срокам реализации проектов и бизнес-задачи? Опираясь на свой 20-летний опыт в области цодостроения, на вопросы «ИКС-Медиа» отвечает исполнительный директор «Ди Си Квадрат» Александр Мартынюк.

– Главное в ЦОДе – надежность. Какие сегодня предъявляются требования к надежности?

– Один из основных новых трендов – появление запросов на комбинированный (гибридный) подход к обеспечению надежности. Речь идет о том, чтобы в рамках одного ЦОДа реализовать разные уровни надежности, задействуя разные архитектуры и технические решения. Правда, подобные запросы пока поступают только от корпоративных клиентов.

Такие клиенты делят ЦОД на несколько зон в зависимости от требований к непрерывности работы ИТ-инфраструктуры. Например, одна зона выделяется для критичных для бизнеса решений – там полноценный Tier III, стандартные системы кондиционирования, бесперебойного питания (с батарейной поддержкой в течение 15 мин) и т.д.

Но всегда есть некритичные приложения. Если они занимают достаточно большой объем (в стойках), то есть смысл создать для них зону с не столь высокими требованиями к надежности. Это могут быть машзалы без чиллерной поддержки: просто фрикулинг (в том числе прямой) с каким-либо вариантом доохлаждения, например, с помощью адиабатики. Для таких зон характерен более широкий диапазон температуры и влажности, зачастую туда устанавливаются более «теплолюбивые» серверы. Все понимают, что в случае экстремально высокой температуры на улице есть риск отключения оборудования в этих зонах. И клиенты к этому готовы. Раньше такого не было.

Также все чаще выделяют зоны коммутации – для подключения к операторам связи, организации соединений между узлами сети ЦОДов и т.д. Такие зоны становятся все обширнее, поскольку растет важность коннективности, в том числе для геораспределенного резервирования.

Подобный комбинированный подход с разделением на зоны разного уровня надежности намного снижает затраты. Система холодоснабжения – это примерно 35% бюджета ЦОДа. Если ее упростить, перейдя к фрикулингу, возможно, с частичной адиабатикой, но без сложной чиллерной системы, можно существенно сэкономить.

– Вы упомянули геораспределенное резервирование. Речь идет о резервировании в сети ЦОДов?

– Да, и это еще одна важная тенденция. У нас сейчас в работе несколько проектов – опять-таки корпоративные объекты, – когда за счет резервирования в сети ЦОДов требования к надежности инженерной инфраструктуры отдельных объектов снижаются.

В качестве примера приведу проект, который предусматривает реализацию трех абсолютно одинаковых ЦОДов. Расстояния между ними таковы, что возможна синхронная репликация данных. Получается, что на всех трех площадках одинаковое не только оборудование, но и данные приложений. Таким образом, три площадки уровня не ниже, чем Tier II, дают в целом систему с уровнем надежности выше, чем Tier III.

В таких проектах очень важна коннективность, каналы связи. Поэтому в них существенное число стоек – десятки – отводится для установки коммуникационного оборудования. Кроме того, в отличие от классических коммерческих ЦОДов, где обычно делают только «инженерку», это комплексные проекты, в которых повышение надежности обеспечивается на уровне ИТ-систем.

– Говоря о надежности, нельзя обойти вниманием появление в России первого коммерческого ЦОДа уровня Tier IV. Подстегнуло ли это запросы на Tier IV?

– Запросы есть. Несколько проектов ЦОДов уровня Tier IV в Москве находятся сейчас в стадии проработки, проектируем ЦОД Tier IV в Казахстане. Но надо понимать, что Tier IV – не такая простая история, как некоторые пытаются представить.

Tier IV налагает серьезные ограничения на архитектурные решения, и далеко не на всех площадках можно выполнить соответствующие требования без существенного удорожания. Даже если это возможно технически, то неясно, будет ли целесообразно экономически. В среднем ЦОД уровня Tier IV на 15–20% дороже, чем Tier III.

Когда заказчик просит Tier IV, важно понимать, для чего, есть ли в этих инвестициях экономическая целесообразность (ибо на проекты коммерческих ЦОДов мы всегда смотрим с точки зрения их окупаемости). Документально подтвердить 20%-ное повышение стоимости услуг на базе Tier IV мы пока не можем. Конечно, наличие ЦОДа Tier IV позволит его владельцу или оператору дистанцироваться от конкурентов. Но вопрос окупаемости остается.

– Рост интереса к искусственному интеллекту породил разговоры о резком повышении мощности стоек. Ряд мировых провайдеров заявили о вводе в эксплуатацию высоконагруженных стоек на 50 и даже 100 кВт. А что запрашивают российские заказчики?

– Если говорить о корпоративных ЦОДах, то все запросы сегодня начинаются от 10 кВт на стойку. Например, один заказчик планирует устанавливать в своем ЦОДе стойки двух типов: на 12 кВт (для систем хранения) и на 18 кВт (для серверов). Другой планирует все стойки – а их больше тысячи – по 11 кВт. Но запросы на стойки более 20 кВт практически отсутствуют. Был один запрос на стойки по 50 кВт, но не из России. Никакого резона в размещении таких стоек на данный момент я не вижу, постараюсь убедить в этом заказчика.

Коммерческие ЦОДы проектируем в среднем на 7,5–10 кВт на стойку, пятикиловаттных проектов сейчас уже нет. Есть один уникальный проект, где рассматриваются стойки 22 кВт, но не для colocation. Локация этого ЦОДа не дает возможности выезда туда заказчиков, поэтому единственный вариант продажи услуг – сдача в аренду вычислительных мощностей, причем с дисконтом: там дешевое электричество. Мы помогаем заказчику проработать финансовую модель, составить бизнес-план.

В целом подавляющее большинство проектов реализуются на базе классического воздушного охлаждения. На данный момент в проработке только один проект с жидкостным охлаждением – как раз со стойками на 22 кВт.

Тенденция высоконагруженных стоек на 50 кВт до нас пока не дошла. Возможно, это обусловлено тем, что нам из-за санкций недоступны самые современные GPU, на базе которых как раз и реализуются такие стойки.

– Как меняются масштабы проектов? Коммерческие ЦОДы, очевидно, становятся все крупнее? А что с корпоративными?

– Масштаб проектов сильно вырос. В 2004 г. мы построили один из первых ЦОДов в России – на 80 стоек, по тем временам очень большой. Еще через 10 лет одна из крупнейших федеральных розничных сетей искала площадку для размещения клона своего европейского ЦОДа, общий объем – 24 стойки на всю федеральную сеть. И это был большой запрос для рынка.

Сегодня же ввод коммерческого ЦОДа на 4000 стойко-мест в Москве не оказывает практически никакого влияния на стоимость стоек на рынке. У нас в работе проекты коммерческих ЦОДов на 4000, 5000, 8000 стойко-мест. Вот такие сейчас масштабы. Это десятки мегаватт мощности, что сильно усложняет подбор площадки, поскольку получить эти мощности очень непросто.

Размеры корпоративных ЦОДов тоже увеличиваются. Но тут я вижу любопытное двунаправленное движение. Компании, которые исторически начинали с постройки своих ЦОДов, сейчас активно арендуют стойко-места в коммерческих ЦОДах, перераспределяя ИТ-ресурсы между собственными и арендными площадями. У этих компаний свои площадки, как правило, небольшие, а вот арендуют они много. С другой стороны, компании, которые всегда арендовали площади в коммерческих ЦОДах (и у которых изначально своих ЦОДов не было), сейчас начинают строить собственные. У них требования к размерам и инфраструктуре совсем другие, они строят ЦОДы намного более крупные, чем те, которые арендовали.

– А как изменились сроки реализации проектов, ведь, как известно, время – деньги?

– Обманывать не буду: сроки увеличились. Реальные сроки постройки ЦОДа на 1000 стоек примерно таковы: 6–9 месяцев проектирование, 15–18 месяцев строительство. С пусконаладкой и сертификацией, как правило, все же 18 месяцев. Получается 2–2,5 года.

Можем ли мы строить быстрее? Конечно. Но для этого должно сойтись много факторов. У заказчика должно быть четкое понимание, чего он хочет. Это понимание должно быть сформулировано, и заказчик не должен его менять. У него должно быть непрерывное финансирование. Должна быть площадка со всеми документами для оперативного получения разрешения на строительство и прохождение коммерческой экспертизы (без обязательного требования госэкспертизы). Должно быть подходящее и устраивающее всех оборудование. Наконец, у исполнителя должны быть ресурсы для выполнения монтажа с той скоростью, которая требуется. Тогда можно уложиться в 12 месяцев, но без предсертификационного тестирования и собственно сертификации. А это еще месяца три.

Последние из названных этапов чрезвычайно важны, ведь наша цель – получить объект, который после подписания актов ввода в эксплуатацию будет готов именно к эксплуатации, а не к доделке, переделке, пусконаладке и доработке. К моменту, когда мы начинаем сертификацию, все работы должны быть завершены. Потом мы запускаем системы и проверяем их функционирование во всех режимах. В рамках commissioning (подробнее про commissioning см. «ИКС» № 3'2023, с. 16. – *Прим. ред.*) проводим нагрузочные испытания – запускаем системы на сутки на полную нагрузку. За сутки выявляются все элементы, которые имеют заводской брак. Их надо изолировать, заменить. Потом заново протестировать. Примерно две недели только тесты – на тысячнике. Потом сертификация – еще дней 10. И после сертификации мы подписываем акт ввода объекта в эксплуатацию, будучи уверенными, что все проверили, все работает.

– Как изменяется отношение заказчиков к ЦОДам? На этот рынок, например, выходят девелоперы, для которых ЦОД – это объект вложений, просто особый вид дорогой недвижимости.

– Да, девелоперы активны, по вопросам цодостроения встречался с представителями десятка компаний, всех основных застройщиков. Они очень эффективны в плане получения энергетики, капитального строительства. Но их задача – построить объект и продать его оператору ЦОДа. Важно качество объекта, насколько он будет ликвиден. А это зависит от того, с какой профессиональной командой они будут сотрудничать. Чтобы команда смотрела на ЦОД как на объект бизнеса.

Лет 10–15 назад о том, как построить ЦОД, я думал прежде всего с инженерной точки зрения. Сейчас, прежде чем переходить к проработке технических решений, мы занимаемся бизнес-вопросами. Если проект не окупится, то проекта не будет. Мы начинаем с заказчиком прорабатывать варианты услуг, формируем воронку продаж, график заполнения ЦОДа, обсуждаем денежный поток, организацию службы продаж. Только потом переходим к технике, позволяющей реализовать проект, который окупится. Идем не от технических решений, а от бизнес-задачи. Это, пожалуй, самое существенное изменение в нашей работе.

Глядя назад, можно с уверенностью сказать, что российские цодостроители прошли большой путь, научились проектировать и строить большие надежные объекты с гарантированным качеством, решать сложные инженерные задачи. Выросли экспертиза, размеры проектов, их сложность... И процесс разгоняется. Дальше будет только сложнее, а значит, интереснее!

ЦОД на российских решениях. Опыт интегратора

Новые требования регуляторов и уход иностранных вендоров укрепляют тенденцию создания ИТ-инфраструктуры на российских решениях. Как использование продуктов отечественных компаний сказывается на процессе построения инфраструктуры дата-центров?

Юрий Барабанщиков, руководитель направления ЦОД, «ЛАНИТ-Интеграция» (ГК ЛАНИТ)

Основные особенности реализации ЦОДов на базе отечественных решений обусловлены тем, что большинство продуктов достаточно «молоды». С одной стороны, это может создавать дополнительные сложности на разных этапах проекта, а с другой – открывает новые возможности.

Подбор оборудования и ПО для дата-центра

Проекты, связанные с модернизацией существующей инфраструктуры компании или с переходом с импортных решений на российские, нередко наталкиваются на сопротивление ее ИТ-команды, которое не всегда проявляется открыто. Такое сопротивление, как правило, вызвано тем, что нужно переучиваться для работы с новыми решениями, которые зачастую предоставляют меньше функциональности, хуже интегрированы друг с другом, страдают разными «детскими болезнями». Также ИТ-руководство компаний обеспокоено необходимостью переноса данных и сервисов с одних продуктов на другие, что в большинстве случаев требует глубокой проработки, наличия «плана Б» и привлечения высококвалифицированных специалистов.

В этом случае хорошей моральной поддержкой и ключом к успеху станет четкий план действий. Такой план или стратегия могут быть разработаны как силами ИТ-специалистов самой компании, так и с привлечением интеграторов. Обычно в план включают следующие этапы:

- анализ рынка;
- создание шорт-листа решений;
- проведение пилотных проектов;
- выбор комплексного решения;
- проектирование и реализация.

Расскажу подробнее, с какими особенностями мы сталкивались на каждом из этапов реализации проекта.

Анализ рынка. Множество схожих по функциям и производительности продуктов, отсутствие исчерпывающих таблиц совместимости, необходимость задействовать несколько отечественных решений разных производителей вместо одного импортного – всё это значительно усложняет выбор программного обеспечения. Вдобавок отечественное ПО развивается достаточно интенсивно, и то, что вчера было только в планах, сегодня может быть уже реализовано. Это сильно влияет на состав компонентов, используемых для инфраструктуры ЦОДа.

В начале анализа бывает трудно определить список требований, которым должны удовлетворять искомые продукты. Зачастую в качестве такого списка берется перечень возможностей эксплуатируемого импортного ПО или оборудования. В результате выясняется, что ни одно российское решение не отвечает всем требованиям к обеспечению функциональности ЦОДа, и тогда нужно решить, что важно, а что нет, и какие запросы могут быть удовлетворены с помощью нескольких отечественных продуктов.

Пилотирование. Как правило, пилотировать приходится больше одного-двух выбранных вариантов. Это обусловливается особенностями предыдущего этапа. Если у вас достаточно ресурсов, то рекомендуется проводить несколько пилотов одновременно – это значительно ускорит процесс реализации и поможет сравнить решения. Возможно, решение, которое не годится для текущего проекта, хорошо подойдет для другого. Если на этапе анализа удалось грамотно расставить приоритеты требуемым функциональным и техническим возможностям, то это значительно упростит разработку программы тестирования и сравнение результатов пилотных проектов.

Выбор решения. Не для всех решений можно определить явного лидера на рынке. В результа-

те пилотов может быть сформирован список решений, которые будут обладать разными достоинствами и недостатками, и сравнить их будет непросто. Помимо пилотных проектов и анализа доступной документации нелишним будет убедиться, что выбранные продукты имеют положительную «кредитную историю», т.е. успешно эксплуатируются в других организациях. Производитель или интегратор могут помочь с поиском компаний, у которых выбранные российские продукты уже установлены, и организовать визит, чтобы лично обсудить особенности их эксплуатации и работу технической поддержки. Также рекомендуется обратить внимание на доступность обучающих курсов для ИТ-команды, которая будет заниматься сопровождением.

Проектирование. На данном этапе все более или менее хорошо, за исключением того, что не у всех российских продуктов есть исчерпывающая документация. Отчасти этот недостаток компенсируется опытом, полученным на пилотных проектах, или опытом исполнителя, если привлекается сторонняя организация. Как и раньше, перед проектированием необходимо определить необходимый и достаточный состав разрабатываемых проектных документов. Не всем организациям нужна документация в строгом соответствии с требованиями ГОСТа. Однако нужно понимать, что наличие качественного рабочего и эксплуатационного пакета документов значительно сокращает сроки внедрения, уменьшает количество возможных ошибок на этапе реализации, упрощает закупочные процедуры, а также позволит в будущем, когда встанет вопрос о модернизации созданной инфраструктуры ЦОДа, обходиться без аудитов или минимизировать их.

Построение инфраструктуры ЦОДа с нуля занимает полгода и больше

Реализация. На этом этапе мы чаще всего сталкивались с двумя проблемами:

1. Служба технической поддержки вендоров аппаратных решений долго устраняет неисправности.
2. Обновления системного ПО, вышедшие с момента проведения пилота до момента реализации, заставляют вносить изменения в проект.

С первым пунктом заметны значительные улучшения, так как большинство производителей инфраструктурного «железа» количественно и качественно усилили команды техподдержки или заключили контракты с крупными сервисными компаниями. Что касается обновлений системного ПО, то нужно заранее позаботиться о получении от производителей дорожной карты развития продукта и выпуска новых версий. Также настоятельно рекомендуется предусмотреть дополнительные аппаратные ресурсы, на которых можно разворачивать и тестировать обновления системного ПО перед их применением в продуктивной среде.

На каждом из этапов важно поддерживать связь с разработчиками решений и продуктов, на которых планируется строить инфраструктуру ЦОДа. Для продуктов, еще не перешедших в разряд коробочных, такая связь обязательна. Плюсом здесь является то, что можно заранее договориться с разработчиком о необходимых функциях или их расширении в соответствии с требованиями конкретного проекта. Безусловно, заказчики с крупными проектами будут у производителей решений в приоритете.

Продолжительность подобных проектов варьируется от восьми месяцев до двух лет в зависимости от сложности и объема.

В проектах, где инфраструктура ЦОДа строится с нуля, меньше привязка к накопленной экспертизе, нет необходимости в проработке процессов миграции, не требуется обеспечивать совместимость с существующими продуктами. Список потенциальных решений обусловливается задачами, которые должен решать ЦОД. В результате выбор оказывается более широким и, можно сказать, более простым. Этапы, скорее всего, окажутся теми же, что и в предыдущем случае, но их длительность и трудоемкость будут значительно меньше.

Интеграторы в большинстве своем имеют хорошее представление о функциях и характеристиках российских решений, регулярно общаются с производителями, проводят собственные тесты и сравнения. Привлечение интегратора на раннем этапе позволит значительно ускорить подбор продуктов для конкретной задачи.

Построение инфраструктуры ЦОДа с нуля занимает полгода и больше. И также зависит от объемов, сложности решаемых задач и количества организаций, вовлеченных в проект.

Из положительных моментов можно отметить создание и развитие экосистем на базе российских решений. Эти процессы идут по-разному: как путем поглощения компаний и встраивания их продуктов в экосистему одного производителя, так и путем развития продукта той или иной компании в разных направлениях, обогащения его функциями смежных продуктов. В результате появляется возможность приобрести продукт у одной компании и далее расширять его возможности дружественными продуктами или покупкой лицензий на дополнительные функции без необходимости проведения пилотных проектов и тестирования. Это сокращает время на выбор решения и тестирование и упрощает использование технической поддержки.

Чек-лист

Для того чтобы при построении ИТ-инфраструктуры ЦОДа избежать ошибок и потери времени, рекомендуется не упускать из виду следующие моменты:

1. **План проведения работ.** Рекомендация, применимая ко всем проектам, в данном случае особенно актуальна. Будьте готовы к тому, что установленные изначально сроки могут существенно «поплыть». Причины банальны: вендор не успевает поставить оборудование, в процессе пилотного тестирования выявляется несовместимость выбранных продуктов и т.п. Защитой здесь может стать проведение нескольких пилотов одновременно, но вы должны иметь возможность привлечь достаточное количество специалистов на время этих работ.

2. **Дата реализации.** Многие проекты переходят в фазу реализации в конце календарного года. Если ваш проект именно такой, нужно заранее позаботиться о бронировании оборудования у производителя и датах поставки. Как правило, на производствах в конце года увеличивается загрузка, и некоторые поставки могут быть задержаны или даже перенесены на следующий год.

3. **География проекта.** Не все производители могут обеспечить высокий уровень технической поддержки по всей территории страны. Если на удаленной от крупных центров площадке постоянно присутствует эксплуатирующий персонал, быстрое восстановление можно обеспечить наличием запасных частей, инструментов и принадлежностей. Но об этом нужно подумать заранее и выбрать оптимальный вариант.

4. **Мониторинг и управление.** Крупные современные ЦОДы не обходятся без централизованных систем мониторинга и управления. Рекомендация здесь следующая: проверьте, что выбранные вами продукты (серверы, системы хранения, системное ПО и прочее) не только совместимы с выбранной системой мониторинга, но и передают в нее всю необходимую информацию о состоянии своих компонентов.

Итак, построить ЦОД на российских решениях вполне реально, хотя это может потребовать более тщательного анализа используемого оборудования и ПО, бóльших временных и трудовых затрат. Однако с ростом числа завершенных проектов, накоплением опыта интеграторов и заказчиков и развитием отечественных решений эти недостатки будут постепенно сглаживаться. ИКС

NED на рынке инноваций для ЦОДов

Предлагая весь спектр классических решений для охлаждения, NED выводит на рынок новые продукты: холодные стены и системы фрикулинга с адиабатическим доохлаждением. Рассказывает Антон Сараев, руководитель направления ЦОД компании NED.

– Компания NED относительно недавно вышла на рынок инженерных систем для центров обработки данных. Чем вас привлек этот рынок?

– Это один из самых динамичных сегментов рынка холодильного оборудования. Системы охлаждения – критически важный элемент инфраструктуры ЦОДов, они обеспечивают необходимые температурно-влажностные условия для надежной работы ИТ-оборудования. Инвестиции в соответствующие продукты быстро увеличиваются. Логично, что мы решили использовать свою экспертизу и наработки в технологиях охлаждения для сегмента ЦОДов.

Компания NED присутствует на рынке 30 лет. Начинали мы с систем вентиляции. Сейчас компания – крупнейший производитель систем охлаждения и вентиляции в России. У нас в штате свыше 2500 человек, из них более 100 конструкторов, которые занимаются исследованиями и разработкой новой продукции. Оборудование NED выпускают две производственные площадки: одна в Подмосковье (город Дзержинский), другая в Белгородской области.

На наших заводах реализован полный цикл производства с максимально возможной локализацией. Если что-то можно производить в России, то мы это производим, в частности, теплообменное оборудование, корпуса, системы автоматики, роторные регенераторы (теплообменные вставки диаметром до 3 м для систем вентиляции), моторно-вентиляторные группы. Думаю, сейчас в России трудно сделать более импортозамещенный продукт, чем делаем мы.

– Какие технические решения вы предлагаете для ЦОДов?

– У нас широкая линейка продукции. Для ЦОДов мы предлагаем все виды рядных и шкафных прецизионных кондиционеров – как на фреоне, так и на воде, а также любые чиллеры: моноблоки, с выносными конденсаторами, с водяным охлаждением, на винтовых и спиральных компрессорах. Наша линейка чиллеров начинается с машин на 30 кВт. Но цодовская линейка – это от 130–140 кВт. Моноблоки выпускаем производительностью до 1,5 МВт, если говорить о чиллерах с выносными конденсаторами – 2–2,5 МВт. Иными словами, у нас есть решения для всего диапазона потребностей ЦОДов, даже самых крупных.

– А какие инновационные системы есть в вашем портфеле?

– Системы, считающиеся инновационными для ЦОДов, часто базируются на компонентах, которые уже давно выпускаются. Одна из таких систем – холодная стена. Собрать холодную стену на основе компонентов, которые у нас уже есть, мы могли и раньше, но теперь это решение становится готовым продуктом со своими конкурентными преимуществами. Здесь важны наши возможности дорабатывать такие решения по требованиям конкретного заказчика, поскольку, как мы знаем, каждый ЦОД имеет свои особенности.

Другое новое решение также реализовано на базе знакомых всем продуктов – приточно-вытяжных вентиляционных установок. Сейчас эти установки используются для создания систем фрикулинга с возможным использованием в них адиабатических доохладителей, но без сложных и дорогостоящих чиллерных систем.

Здесь следует сказать о кардинальном изменении отношения заказчиков к системам фрикулинга. В этом году мы получаем огромное число запросов на такие системы. Раньше этого не было. Все больше заказчиков готовы мириться с увеличением температуры в машзалах ради повышения энергоэффективности и существенного снижения капитальных и операционных расходов. Причем подобные запросы поступают не только от корпоративных, но и от коммерческих ЦОДов.

Интересно также отметить, что большая часть (примерно три четверти) запросов поступает на системы прямого фрикулинга, четверть – на косвенный фрикулинг (когда воздух с улицы не подается в машзалы, а охлаждает в теплообменниках воздух, циркулирующий внутри ЦОДа). Более того, если климат в месте размещения ЦОДа и характеристики ИТ-оборудования позволяют, заказчики просят системы полного фрикулинга вообще без доохладителей. При необходимости к секции адиабатического охлаждения можно добавить фреоновый доохладитель или доохладитель на охлажденной воде.

Сейчас мы дорабатываем свои решения на базе приточно-вытяжных вентиляционных установок: повышаем уровень герметичности, увеличиваем единичную мощность и т.д. Как и в случае с холодными стенами, планируем в скором времени представить отдельную линейку готовых продуктов.

Как видите, мы производим весь спектр классических систем охлаждения для ЦОДов и, наверное, 80% специализированных решений.

– Насколько требования заказчиков-ЦОДов отличаются от требований заказчиков из других отраслей?

– ЦОДы предъявляют повышенные требования к надежности и рабочим характеристикам оборудования. Более то-

го, заказчики из этой сферы очень грамотны, зачастую они лучше всех знают, какое решение им нужно, – лучше нас, производителей, лучше проектировщиков, лучше генподрядчика. Они более четко и профессионально формулируют технические требования. Для заказчиков из других отраслей мы обычно выступаем экспертами. Цодовский заказчик часто сам главный эксперт.

Мы это быстро поняли и поэтому, по крайней мере на текущем этапе работы с ЦОДами, не навязываем свои компетенции. Предпочитаем сделать так, как хочет заказчик, поскольку он чаще всего действительно знает, как лучше. Мы готовы прислушиваться и кастомизировать свои продукты.

Кастомизация – важный момент. Те же холодные стены и решения с фрикулингом на базе приточно-вытяжной вентиляции – это большой конструктор. Из него можно собрать систему, отвечающую почти любым требованиям, учитывающую особенности здания и помещений, климата в месте развертывания ЦОДа, специфику ИТ-оборудования и т.д. Мы готовы подстраиваться, даже на этапе производства, и делаем это: дорабатываем систему, проводим необходимые тесты, чтобы на 100% выполнить требования заказчика.

– Сейчас растет спрос на высокоплотные решения, в связи с чем заказчики задумываются о прямом жидкостном охлаждении. Предлагает ли NED такие решения?

– У нас в компании есть серьезная экспертиза по жидкостному охлаждению, мы готовы создавать решения практически для любой плотности тепловыделения. Но пока не видим реального спроса. Да, плотности растут, но не такими темпами, чтобы говорить о существенной доле оборудования, которому необходимо жидкостное охлаждение. Однако подчеркну, мы знаем, как реализовать эти решения, и готовы к этому.

– Сотрудничаете ли вы с другими производителями, чтобы предлагать заказчикам комплексные решения?

– Мы работаем в партнерстве с поставщиками стоек, систем изоляции коридоров, источников бесперебойного питания. Это помогает нам лучше понять, что нужно заказчику. Более того, когда мы знаем, например, высоту коридора, тепловыделение ИБП и другие характеристики, это позволяет оптимизировать решение нашей основной задачи – охлаждения оборудования.

О NED важно знать следующее: мы – производитель холодильного оборудования и не занимаемся перепродажей стороннего оборудования. Мы можем помочь заказчику проработать полное решение, подготовить спецификацию на такое оборудование, но сами не продаем его. К тому же, по моим наблюдениям, сейчас спрос на комплексные решения «из одних рук» снижается.

– Как у вас организовано техническое обслуживание оборудования? Насколько близко вы находитесь к площадкам заказчиков?

– У нас одна из крупнейших сервисных сетей. В каждом городе-миллионнике есть представительство NED и склад запчастей для проектов, реализованных в данном регионе. Сервисные представительства есть и в ряде городов поменьше. Охватываем всю Россию от Калининграда до Приморья. Это позволяет нам предлагать сервисные контракты практически любого уровня. Скажем, в Москве мы готовы обеспечить время реагирования 4 часа. Понятно, что для удаленных площадок время реагирования во многом определяется транспортной доступностью. Для того чтобы уменьшить его, мы бесплатно обучаем заказчиков эксплуатации оборудования и готовы обучать партнеров обслуживанию и пусконаладке всей нашей линейки. По всей стране у NED есть тысячи партнеров, которые могут поддерживать и сопровождать наше оборудование.

Также отмечу, что при стандартной гарантии на оборудование 3 года у нас есть опция расширенной гарантии – 5 или 7 лет.

– Можете привести примеры проектов, реализованных для ЦОДов на базе решений NED?

– Проектов много, но в большинстве случаев мы не можем называть заказчиков. NED постоянно ведет крупные поставки для корпоративных ЦОДов. За год мы поставили на этот рынок сотни рядных кондиционеров, чиллеры общей производительностью десятки мегаватт.

Например, наши чиллеры (на несколько мегаватт) установлены в новом коммерческом дата-центре компании Key Point в Новосибирске. Континентальный климат, когда температура зимой может опускаться до −50°C, а летом подниматься до +37°C, потребовал от нас расширить температурный диапазон эксплуатации чиллеров. Мы успешно справились с этой задачей. У Key Point амбициозная программа развития региональной сети ЦОДов, и сейчас мы прорабатываем возможность использования нашего оборудования в других городах.

– Каковы планы развития цодовского направления?

– Как я уже говорил, на текущем этапе мы больше слушаем ЦОДы, делаем то, что они просят. Но в перспективе, с учетом нашей экспертизы и производственных возможностей, хотим предлагать решения, которые будут превосходить текущий уровень. Хотим формировать тренды, в какой-то мере опережать конкурентов по выводу на рынок новых продуктов.

Конечно, работаем над повышением узнаваемости бренда NED на рынке ЦОДов. И видим, как ситуация меняется: еще год назад нас мало кто знал, теперь знают хорошо.

Продажи наших продуктов для ЦОДов сейчас увеличиваются примерно на 20% в год, что соответствует динамике рынка ЦОДов в целом. Надеемся увеличить темпы нашего роста, в том числе благодаря новым продуктам.

Среда общих данных как основа BIM/ТИМ

Геннадий Дрягин, BIM-менеджер, «Свободные Технологии Инжиниринг»

При работе над проектом с использованием технологий информационного моделирования среда общих данных помогает упорядочить внутренние процессы и согласование документов, благодаря чему существенно повышается эффективность работы и снижаются проектные издержки.

Для чего нужна СОД

Аббревиатура BIM (в русскоязычном варианте ТИМ, т.е. технологии информационного моделирования) чаще всего расшифровывается как Building information modeling. Но есть и другое прочтение: Building information management. Различия в последнем слове определяют разные подходы. В первом мы только создаем информацию, а во втором мы ей управляем. К сожалению, внедрение BIM в строительную отрасль для многих ее участников происходило и до сих пор уверенно происходит только на уровне применения специального программного обеспечения для создания информационных моделей. Методология обмена информацией и совместного управления данными зачастую упускается из виду.

В результате в компаниях подробно описаны принципы работы с инструментом разработки информационных моделей, а вся остальная проектная информация хранится, передается и согласуется бессистемно. Под проектной информацией понимается любой документ, комплект документов, информационная модель или их совокупность, а также иные проектные данные. Поскольку информация может быть представлена в разных видах, ее обобщенно называют информационным контейнером.

Один из способов организации единого пространства для хранения, передачи и согласования информационных контейнеров – это создание среды общих данных (СОД) и описание методик ее работы.

СОД – совокупность программно-аппаратных и методологических средств, направленных на создание и описание взаимодействия между участниками проекта. Подчеркнем, что внедрение СОД не заканчивается выбором и развертыванием того или иного программного решения. Применение СОД без должного изменения и описания процессов хранения информации и обмена ею будет эквивалентна простому хранению в любом из файлообменников.

Рассмотрим обмен информацией между участниками любого из этапов проектирования и строительства (рис. 1). По идее он представляет собой последовательный процесс передачи, согласования, возврата и комментирования информационных контейнеров. Но на деле процесс зачастую выглядит как хаотичное перенаправление разных версий конейнеров с возможной потерей их частей.

При передаче информации от одного участника к другому изменяются версии некоторых документов, добавляются комментарии (замечания и ответы), ряд документов проходит согласование, другие возвращаются на доработку. Когда в эти процессы вовлечены все проектные документы, относящиеся к одному объекту, может произойти информационный коллапс, в котором

Рис. 1. Пользователи среды общих данных

отследить актуальность и путь информационного контейнера практически невозможно (рис. 2).

Ключевые функции СОД

Программное решение СОД должно поддерживать несколько основных функций:

- хранение информации;
- поддержка версионности информации;
- взаимодействие с информацией;
- создание маршрутов движения информации.

Хранение информации

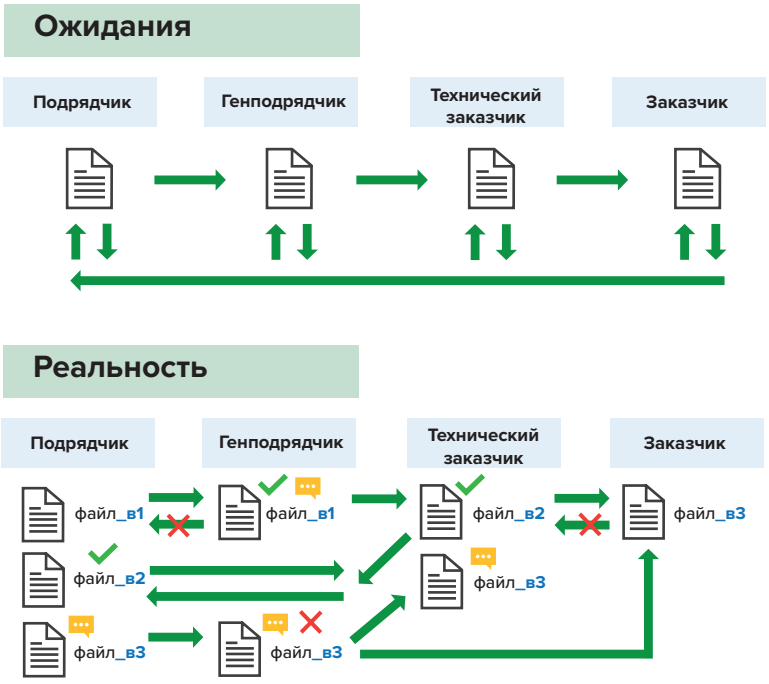
Когда мы говорим о хранении, чаще всего имеем в виду физический уровень. Для многих компаний при выборе такого рода систем достаточно важно, где будут находиться аппаратные средства, на которых развернута СОД. На рынке представлены как on-cloud, так и on-premise решения. Второй важный момент – резервирование аппаратных средств. В облачных решениях резервирование чаще всего обеспечивается поставщиком или разработчиком системы, а в локальных ложится на плечи внутренней ИТ-службы.

Так как СОД – это единая площадка для многих участников проекта, необходимо, чтобы выбранная система позволяла гибко разграничивать доступ к тем или иным зонам, ресурсам и информационным контейнерам. Одни участники должны иметь возможность как загрузки, так и редактирования информации, а другим достаточно чтения. При этом часто нужно разделять пользователей по их компаниям, отделам, проектным ролям.

Особо выделяются СОД, которые позволяют взаимодействовать с BIM-данными, причем не только хранить, но также просматривать и анализировать компоненты информационных моделей. Загрузка информационных контейнеров с BIM-данными в СОД осуществляется как через форматы разработки информационных моделей, так и через промежуточные форматы (рис. 3). В качестве общепринятого интероперабельного формата чаще всего используются файлы спецификации IFC.

Отслеживание версий

Версионность информационных контейнеров зачастую поддерживается по умолчанию. Однако можно выделить несколько подходов. Самый простой и распространенный – указание номера версии в формате 1, 2,... n в качестве дополнительного атрибута контейнера. Менее распространено, но достаточно подробно описано в международном документе ISO 19650 масочное формирование версий, при котором указываются текущая зона хранения и статус контейнера (рис. 4). Рассмотрим пример со следующими зонами:



▲ **Рис. 2. Ожидаемое и реальное движение проектной информации между участниками проекта**

- Зона рабочих данных (WIP, Work in Progress). Область СОД для хранения текущих данных одной из групп участников проекта. Информация в зоне WIP доступна только конкретной группе участников.
- Зона общих данных (Shared). Область СОД, где материалы участников проекта хранятся в общем доступе для смежных подразделений и контрагентов.
- Зона опубликованных данных (Published). Область СОД, куда выкладываются готовые, утвержденные материалы для передачи контрагентам или заказчику.

В этом случае на основе выбранной кодификации можно получить достаточно подробную информацию об элементе информационного контейнера.

Просмотр данных и взаимодействие с контейнером

Хранения информационных контейнеров и поддержки их версионности недостаточно. Еще одна необходимая функция – доступ для просмотра информационных контейнеров или взаимодействия с ними. Стандартные форматы,

Рис. 3. Загрузка информационных контейнеров с BIM-данными в СОД ▼

▲ **Рис. 4.** Масочное формирование версий

предназначенные для просмотра, – векторные PDF, XPS или растровые JPEG и PNG. Некоторые документы (тексты, таблицы и т.п.) зачастую не подлежат редактированию в системе СОД, так как это выходит за рамки основных функций системы и требует специальных редакторов. Многие системы поддерживают работу с информационными контейнерами, содержащими BIM-данные, на уровне сведения их компонентов и предоставляют отдельный инструмент для их просмотра. Некоторые системы поддерживают связку информационных контейнеров в СОД с различными графиками проектирования или производства работ, что позволяет более гибко использовать эти системы и более тесно интегрировать данные между собой.

Взаимодействие с информационными контейнерами, загруженными в СОД, подразумевает не только их просмотр, но и добавление новой информации, а также их связку. Сюда можно отнести инструменты комментирования и создания замечаний. При просмотре содержащего графическую информацию контейнера непосредственно в системе СОД можно создать дополнительные компоненты в виде графических или текстовых элементов, которые в дальнейшем существуют в СОД как связанные с выбранным контейнером сущности. Эти сущности также хранятся, поддерживается их версионность и согласование с выделенными маршрутами и ответственными. Некоторые СОД могут выполнять проверку изменений в разных версиях загружаемого контейнера, что дает возможность отслеживать жизненный цикл контейнера в СОД.

Создание маршрутов движения информации

Согласование информационных контейнеров строится на основе различных маршрутных карт. Чем больше вариантов таких карт, тем более гибкие сценарии можно использовать. Иногда достаточно обеспечить последовательное согласование несколькими пользователями, но чаще всего это сложные процессы с различными ролями и группами пользователей (рис. 5). При этом на каждом из этапов согласования могут появляться дополнительные комментарии, а информационные контейнеры могут возвращаться обратно.

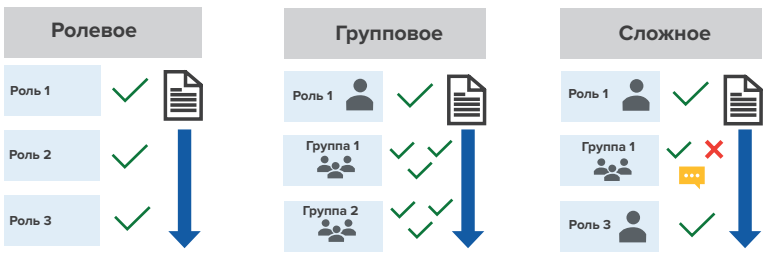


Рис. 5. Варианты согласования информационных контейнеров ▼

Некоторые СОД при согласовании контейнеров поддерживают работу с электронной цифровой подписью (ЭЦП), а также нанесение на графические документы штампов или QR-кодов. Это позволяет даже при переводе информации в «бумажный» вариант сохранять связку с СОД.

Дополнительные функции

Поскольку системы СОД по сути своей – базы данных, большая часть из них имеет возможности анализа информационных контейнеров, процессов или замечаний. Ряд разработчиков СОД предоставляют API для пользовательского анализа данных или интеграций. Другие же имеют собственные модули для демонстрации отчетов и графиков. Раньше я бы сказал, что аналитика – это дополнительная функция, но она уже давно из тренда превратилась в полноценный инструмент работы с данными. А данных у вас может быть очень много. В проектах зачастую участвуют десятки компаний, сотни специалистов, и все они выпускают тысячи страниц с комментариями, изменениями и пр. Если все эти тысячи помножить на число проектов в портфеле, то результат получится внушительный.

Для привлечения новых пользователей разработчики СОД интегрируют в свои системы различные дополнительные модули. Для некоторых компаний эти модули могут заменить или дополнить их собственные цифровые решения. Плюс таких инструментов заключается в том, что зачастую они позволяют связывать данные различных сущностей (документы, графики, стоимости и т.п.) из разных источников. Тем самым польза от систем увеличивается.

Сегодня системы СОД представлены на рынке достаточно широко. При этом мы можем смело говорить не об импортозамещении зарубежных решений, а о наличии широкого выбора отечественных систем, которые давно конкурируют между собой, имеют внушительный пакет внедрений и активно развиваются.

Упорядочение внутренних процессов может существенно повысить эффективность обмена информацией и снизить проектные издержки. Чем больше проектов ведет организация и чем значительнее ее роль в проекте, тем важнее контроль за актуальностью и составом проектных данных. 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

Еще раз про DCIM

Усложнение инфраструктуры, рост требований к надежности и скорости предоставления услуг, дефицит квалифицированных кадров – все это повышает заинтересованность в зрелых системах DCIM, обеспечивающих учет и планирование основных ресурсов ЦОДов.

Евгений Кривоносов, генеральный директор, «СДИ Софт»

Сергей Довгань, технический директор, «СДИ Софт»

«ИКС»: Давайте определим, что понимать под DCIM – слишком уж по-разному трактуют эту аббревиатуру.

Евгений Кривоносов: Да, почти каждый разработчик связанного с дата-центрами ПО называет его DCIM. Программа управления кондиционером – DCIM, программа мониторинга ИБП – тоже DCIM…

Но чего ждут от DCIM заказчики? В первую очередь они хотят иметь полную и достоверную информацию о том, что у них находится в ЦОДах. Это и физические ресурсы, и логические сущности. Важно понимать, как они между собой связаны, каково их текущее состояние, уровень потребления, оценка изменений в будущем. Под основными ресурсами инженерной инфраструктуры понимают свободное место, доступную электрическую мощность, холод и портовую емкость.

Сергей Довгань: Зайду немного с другой стороны. Службы эксплуатации ЦОДов всегда стараются автоматизировать свою работу. Здесь возникают три группы задач. Первая – учет и планирование ресурсов, о чем говорил Евгений. Вторая – мониторинг установленного оборудования. И третья – управление работами, плановыми или аварийными.

Системы DCIM в первую очередь решают именно задачи учета и планирования, позволяя контролировать все объекты эксплуатации, связи между ними, области ответственности. Для других задач – мониторинга и управления работами – используют другие инструменты, которые в проектах могут интегрироваться с системой DCIM.

«ИКС»: Учет и планирование ИТ-ресурсов – это часть DCIM или нет?

Е.К.: Корпоративным и государственным ЦОДам важнее учитывать именно ИТ-оборудование: серверное хозяйство, СХД, телекоммуникационное оборудование. А уже потом – инженерная инфраструктура. В наших проектах для таких клиентов уклон в сторону ИТ-оборудования очень сильный, и его учет – обязательная часть DCIM.

В коммерческих ЦОДах ситуация иная. Они идут от «инженерки», поскольку у них граница ответственности часто проходит по блоку PDU, куда подключается оборудование заказчика. ИТ-оборудование находится вне зоны ответственности многих операторов коммерческих ЦОДов.

«ИКС»: Принято говорить, что ЦОДы продают надежность. Как DCIM помогает ее повысить?

С.Д.: Повышение надежности достигается за счет того, что благодаря DCIM сотрудники службы эксплуатации могут быстрее разобраться, где что у них установлено, как подключено, и в случае аварийной ситуации быстрее провести диагностику. На надежность влияет и планирование рутинных задач. Чем больше в зоне ответственности того или иного специалиста объектов (стоек, оборудования и пр.), тем выше вероятность ошибок. Ему нужен инструмент, который должен подсказать, можно ли установить сервер в данную стойку или туда лучше не ставить, потому что не хватит места, портов или чего-либо еще. Наш инструмент предотвращает ошибки, связанные с планированием.

Недавно один заказчик – у которого много ЦОДов, большой штат службы эксплуатации, – пожаловался, что средний срок работы сотрудника в организации три года. За короткое время он должен разобраться в большом хозяйстве, которое ему поручено эксплуатировать, а затем передать эту информацию тому, кто придет на его место. Без инструмента, который позволит быстро войти в курс дела, безошибочно выполнять рутинные операции по перемещению, подключению и планированию, сейчас обойтись почти невозможно. А руководителя такой инструмент защитит от потери больших объемов критичной информации об инфраструктуре ЦОДа, которая хранилась в голове покинувших компанию специалистов.

«ИКС»: Другая важная задача ЦОДа – эффективно использовать основные ресурсы. Как в этом помогает DCIM?

Е.К.: Раньше в контексте инженерной инфраструктуры рассматривали три основных типа ресурсов: электричество, холод и пространство. Сейчас почти каждый заказчик включает в требования также проверку наличия свободных портов для подключения оборудования. Потому что электричество, холод и место могут быть в наличии, но если порты отсутствуют, то оборудование не подключить.

Наша система позволяет получить информацию по этим четырем типам ресурсов «на кончиках пальцев», в одном интерфейсе. Другой важный функционал – анализ доступных ресурсов с целью определить, куда лучше поставить оборудование. Не нужно самому перебирать сотни стоек, система проделает эту работу за вас и предложит оптимальный вариант.

С.Д.: Другой сценарий: пользуясь информацией, которая есть в нашей системе, можно оценить загрузку стоек по разным ресурсам и попытаться, переставив оборудование, использование ресурсов оптимизировать. Это позволяет, например, более плотно установить серверы, высвободив место для дополнительных устройств.

Еще один пример касается долгосрочного планирования. Большая компания, быстро развивается, надо регулярно

строить новые ЦОДы, но делать это вовремя – если загодя, то деньги будут заморожены, если чуть позже, то бизнес-потребность будет реализована с задержкой. Важно оценивать степень загрузки существующих ЦОДов, чтобы за 6–9 месяцев запустить строительство следующего машзала или ЦОДа. Наша система позволяет помочь в решении этой задачи.

«ИКС»: Каковы требования к инфраструктурному оборудованию ЦОДа для работы системы DCIM?

С.Д.: Наша система учетная, поэтому особых требований нет. На первом этапе информация часто вносится вручную. Даже если получается автоматически загрузить ее из других систем, она должна быть верифицирована и авторизована (фактически подписана) ответственными лицами. Это важно, поскольку на основании этой информации принимаются управленческие решения.

На втором этапе обычно выполняется интеграция с другими системами, в частности с системами мониторинга, которые выступают потребителем нашей информации. Если происходит авария, нужно быстро определить, насколько критично отказавшее устройство, что от него зависит. Система мониторинга автоматически получает соответствующие данные из нашей системы и предоставляет их операторам дежурной смены.

Е.К.: Часто реализуем интеграцию с системой управления работами. Сначала необходимые изменения планируются в нашей системе, она проверяет наличие необходимых ресурсов, совместимость модулей, доступность портов, электричества и пр. После этого формируется последовательность технических операций, которая передается в систему управления работами. Как только определенная операция выполняется, нажатием на кнопку она переводится из плановой в актуальную. Помимо всего прочего, на время выполнения работ система еще и забронирует ресурсы, чтобы никто другой не мог их занять.

«ИКС»: Для каких ЦОДов DCIM наиболее актуальна?

Е.К.: Потребность в нашей системе возникает в организациях, у которых есть хотя бы две площадки и несколько сотрудников, которые отвечают за распределенную систему. Они должны понимать, где что стоит и как подключено. Возникает потребность в централизованной системе учета.

Если человек отвечает только за кабели, то ему, возможно, подойдет более простая, узкоспециализированная система. Но если в его зоне ответственности вся «инженерка», то ему нужна функционально насыщенная система, подобная нашей.

С. Д.: Приведу простой пример. Начинаем с того, что документируем площадки. Опрашиваем специалистов, отвечающих за серверы, они перечисляют площадки. Потом то же просим сделать сетевиков. Сравниваем два списка – не совпадают. Люди, у которых оборудование стоит в одних и тех же стойках, по-разному называют площадки. В случае аварии надо быстро разобраться, где и что произошло, а вы не можете сказать, на какой площадке это случилось. Нужна единая база, которая одинаково понимается всеми.

«ИКС»: Можете привести примеры проектов, где уже успешно используется ваша система?

Е.К.: Продолжается один из крупнейших проектов – паспортизация ЦОДов компании МТС. В контуре проекта несколько десятков ЦОДов, рамочное соглашение на 10 тыс. стоек. Мы активно обучаем специалистов МТС, двигаемся к тому, чтобы максимально наполнить систему актуальными данными. МТС также использует нашу систему для планирования строительства новых модульных ЦОДов.

Другой пример – ФКУ «Налог-Сервис» ФНС России, у которой несколько ЦОДов, более 3 тыс. стоек. Скрупулезный заказчик, ему требуется детальное документирование. Интегрируем свою систему с системами мониторинга, управления работами. Проект находится в финальной стадии реализации.

Третий пример – казахстанский оператор «КазТрансОйл», эксплуатирующий нефтепровод, вдоль которого много необслуживаемых узлов связи. Периодически эти узлы посещают инженеры, проверяют, выполняют определенные регламентные работы. Одно из заданий – проверить, что оборудование подключено как положено. Информация для этого, в том числе визуальная, загружается из нашей системы учета.

«ИКС»: Как меняются рынок и отношение заказчиков к системам DCIM?

Е.К.: Рынок растет. Заказчики, которые раньше довольствовались решениями, подобными Excel, Visio, программами open source, сейчас переходят к промышленным решениям. Причин несколько: усложняется инфраструктура, растут требования со стороны бизнеса к надежности и скорости предоставления услуг. Если раньше были свободные руки, чтобы поддерживать те же программы open source, то сейчас все чаще проявляется дефицит кадров. Мы эту тенденцию ощущаем по росту числа запросов.

При выборе продукта заказчикам все важнее становится его технологическая готовность к применению в крупных структурах. Им нужно, чтобы система могла задокументировать, во-первых, все, что связано с инженерной инфраструктурой, во-вторых, все ИТ-оборудование, в-третьих – все кабельные подключения. Плюс обеспечить возможность бесшовного объединения этих блоков информации. Ведь когда происходит авария, надо быстро проверить все эти системы. Важно еще, чтобы продукт можно было быстро развернуть и начать им пользоваться. Ну а дальше уже можно его кастомизировать под специальные сценарии.

Коротко про «СДИ Базис»

Изначально специалисты, которые впоследствии основали компанию «СДИ Софт», сотрудничали с известным немецким производителем (FNT GmbH), одним из лидеров на рынке DCIM. Команда российских программистов росла, и постепенно большая часть кода модуля DCIM стала создаваться именно в РФ. После событий 2014 г. ряд заказчиков обратился с просьбой локализовать продукт. Трансфер технологий шел пять лет, с 2014 по 2019 гг., причем российская компания получила зрелый продукт с сотнями внедрений. На сегодня у «СДИ Софт» не только исходный код, но и все юридические права на технологии, а также производственная база, группа технических экспертов для поддержки заказчиков и сеть партнеров с экспертизой внедрения. «СДИ Базис» – полностью отечественное программное решение, внесенное в единый реестр российского ПО.

Виртуализация сети: от VLAN до VPN

Николай Носов

Эволюция информационных технологий сопровождается изменениями подходов к организации компьютерных сетей.

Виртуальная локальная сеть

В начале 90-х в банке, где в то время я работал в ИТ-отделе, сеть была «плоская» – рабочие станции и серверы подключались к одному неуправляемому коммутатору Ethernet. При подключении сетевого принтера, компьютера или другого устройства к коммутатору в его таблице коммутации, отражающей соответствие портов и MAC-адресов, после поступления на порт первого кадра прописывался уникальный MAC-адрес нового устройства (рис. 1). Пакеты между устройствами пересылались в соответствии с таблицей.

Проработала такая схема недолго – до тех пор, пока имевший сына-программиста шофер банка не поменял через свой компьютер коэффициент потребления топлива в таблице расчета выплат за пробег машины на компьютере бухгалтерии. В то время бухгалтеры не верили компьютерам слепо и через некоторое время заметили, что за тот же пробег шофер стал получать денег на бензин больше.

Мошенничество вскрылось, и ИТ-отделу выделили деньги на недавно появившиеся на рынке управляемые коммутаторы. После чего единую сеть Ethernet разделили на несколько логических сетей, подключенных к разным портам управляемого коммутатора, организовав виртуальную сеть (VLAN). Теперь не имеющие доступа сотрудники в принципе не могли попасть в сегмент сети с сервером бухгалтерии.

Часть портов управляемого коммутатора выделили бухгалтерии, часть – для подсети руководства, по одному – на операционистов, ИТ-отдел и прочих сотрудников. Это позволило создать изолированные на канальном уровне (L2) виртуальные сети (пример подобной сети показан на рис. 2). Кадры Ethernet, поступающие с компьютера главного бухгалтера, допустим, на десятый порт коммутатора, который приписан к VLAN10, автоматически маркировались: к ним добавлялось поле Tag с идентификатором (номером) VLAN (рис. 3).

Далее коммутатор в своей таблице коммутации среди портов, принадлежащих VLAN10, искал порт, к которому подключено устройство с MAC-адресом получателя. Если получатель был подключен к порту того же коммутатора, то тег удалялся и кадр отправлялся в нужный порт таким, каким был изначально, – получателю незачем знать о существовании VLAN.

Если же искомый порт был транковым (магистральным), то тег у него оставался. Через транковые порты кадр передавался на другой управляемый коммутатор, где также искались MAC-адреса устройств, принадлежащих VLAN10. Пакеты заканчивают жизнь на сетевых картах компьютеров или на портах маршрутизатора. Один сегмент VLAN – один широковещательный домен.

Подключение к интернету

Руководство банка долго не разрешало использовать в работе интернет, опасаясь утечек конфиденциальной информации. Но технический прогресс не остановить, и один выделен-

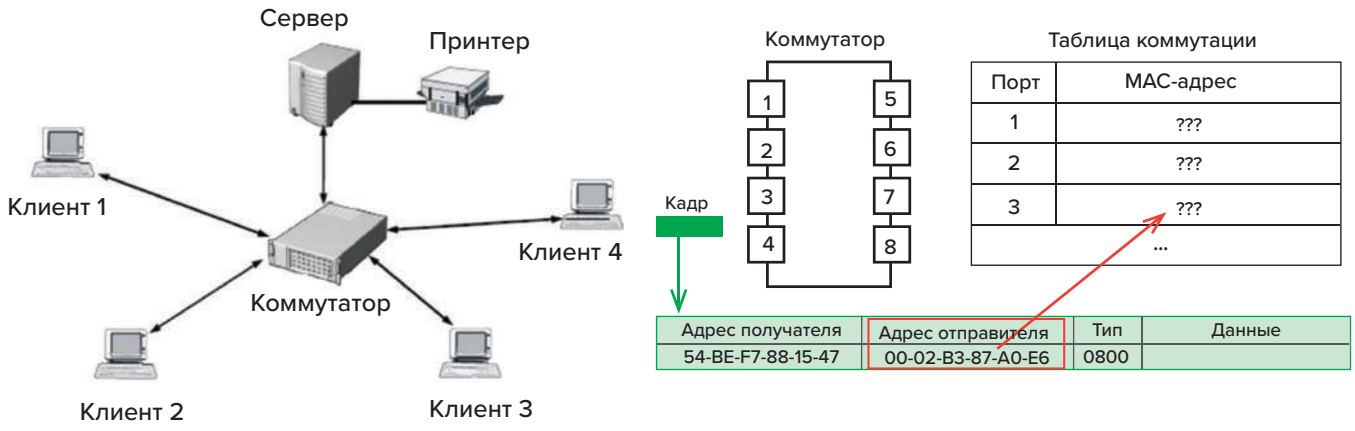


Рис. 1. «Плоская» сеть и таблица коммутации ▼

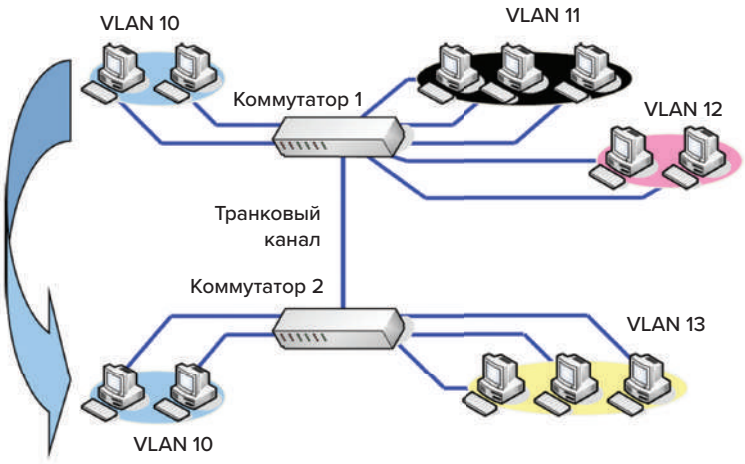
ный компьютер в ИТ-отделе все же подключили к Глобальной сети. Остальные сотрудники банка тоже хотели получать электронную почту и иметь доступ к необходимым по работе сайтам, поэтому пришлось прокладывать параллельную сеть, которая из соображений безопасности даже на физическом уровне не имела связи с основной сетью банка.

Работать с двумя компьютерами на рабочем месте было неудобно, да и изоляции достичь не удалось – данные перетаскивали между сетями на дискетах, а с ними в банковскую сеть попадали вирусы. В итоге параллельная сеть трансформировалась в демилитаризованную зону (DMZ, отдельный защищенный межсетевыми экранами сегмент VLAN) общей физической сети, а сама сеть банка приобрела классическую трехуровневую архитектуру (рис. 4), где основные потоки данных шли по направлению «север – юг» – от компьютеров сотрудников к серверам или выходу в интернет.

Уровень доступа отвечал за подключение компьютеров сотрудников, уровень распределения «разбрасывал» их по VLAN. Уровень ядра, реализованный на двух (для резервирования) самых мощных коммутаторах, обеспечивал быструю передачу данных.

Взаимодействие новой сети с интернетом осуществлял роутер (маршрутизатор), работавший на уровне L3 модели OSI. Основная задача сетевого уровня – создание составных сетей, построенных на основе сетевых технологий разного канального уровня, таких как Ethernet, Wi-Fi, MPLS. Различия технологий приводят к проблемам нестыковки – например, не совпадают максимальные размеры кадра (MTU). Так, в сети Ethernet MTU – 1500 групп из восьми битов, а в сети Wi-Fi – 2300. Различается и адресация. Скажем, в сети Ethernet используется широковещательная.

Для того чтобы согласовать адресацию на сетевом уровне, используются глобальные адреса (IP-адреса), которые не зависят от адресов конкретных технологий канального уровня. Межсетевой протокол (IP, Internet Protocol) объединяет сегменты сети в единую сеть, обеспечивая доставку пакетов данных между любыми узлами сети через произвольное число промежуточных узлов – маршрутизаторов.



▲ **Рис. 2. Организация виртуальных локальных подсетей**

Сетевой уровень решил проблему масштабируемости. Работа велась не с отдельными адресами, как на канальном уровне, а с блоками адресов. Пакеты, для которых путь следования неизвестен, отбрасывались, а не пересылались обратно на все порты.

Виртуальные частные сети

С появлением у банка филиалов возникла проблема обмена данными с ними. Вначале курьеры возили дискеты с запросами и отчетной информацией, благо филиалы были не так далеко. Потом появились дорогие выделенные каналы. С подключением банка к интернету стало возможным значительно удешевить обмен: для безопасного соединения устройств через общедоступные сети начали использовать технологию виртуальных частных сетей (VPN), т.е. создания поверх сети интернет виртуального туннеля, защищающего информацию от несанкционированного доступа.

Обычный (немаркированный) кадр

Адрес назначения (DA)	Адрес источника (SA)	Данные (Data)	Контрольная последовательность кадра (CRC)

Маркированный кадр 802.1p/802.1Q

Адрес назначения (DA)	Адрес источника (SA)	**Тег (Tag)**	Данные (Data)	Контрольная последовательность кадра (CRC)

Идентификатор протокола тега (TPID) 0×8 100	Приоритет (Priority)	Идентификатор канонического формата (CFI)	**Идентификатор VLAN (VID)**
16 битов	3 бита	1 бит	12 битов

◀ **Рис. 3. Обычный и маркированный кадры**

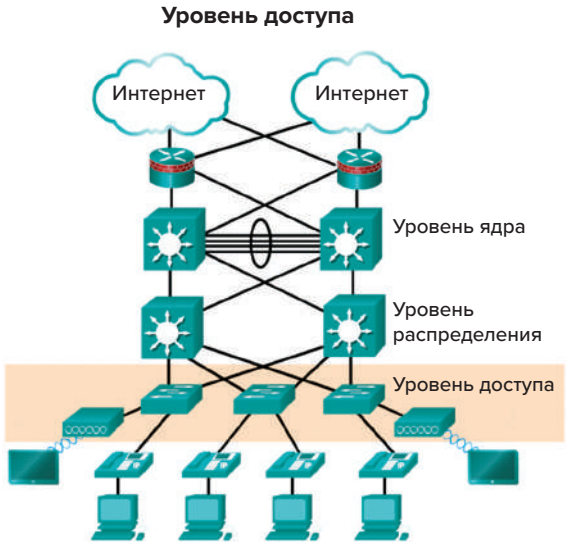


Рис. 4. ▶ Трехуровневая архитектура сети

До туннелирования сетевой пакет состоит из данных и двух определяющих передачу служебных частей:

- Original IP Header. Содержит информацию о версии IP (v4 или v6), исходном IP-адресе и IP-адресе назначения.
- TCP Header. Содержит параметры и информацию о состоянии сквозного TCP-сокета (программного интерфейса). Среди них: номера портов отправляющего и принимающих устройств; номер сегмента TCP; номер, используемый получателем для запроса следующего сегмента TCP; длина заголовка; флаги подтверждения, установления и завершения соединений; контрольная сумма.

При туннелировании оригинальный сетевой пакет встраивается (инкапсулируется) во внешний: добавляется поле Outer IP Header – внешний заголовок IP, содержащий информацию о версии протокола, длине заголовка, типе обслуживания, общей длине пакета, идентификаторе и флагах (рис. 5).

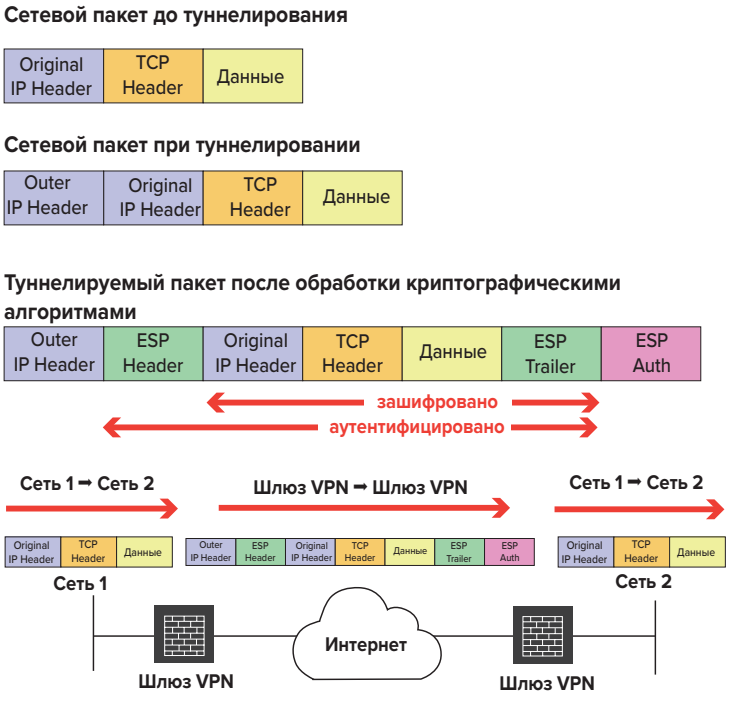


Рис. 5. Общая схема туннелирования сетевого трафика ▼

Для защиты данные, передаваемые по туннелю через интернет, шифруются и в пакет добавляются поля ESP Header, ESP Trailer, ESP Auth. Протокол ESP позволяет комбинировать несколько служб безопасности, таких как обеспечение конфиденциальности данных посредством шифрования, аутентификация пакетов, целостность данных и уникальность пакетов. Технология основана на стеке протоколов: IKEv2 – на уровне control plane, обеспечивающем согласование выбора алгоритма шифрования, аутентификации и контроля целостности; IPSec на уровне data plane осуществляет шифрование оригинальных пакетов и туннелирование средствами протокола ESP. Передачу данных по виртуальному каналу можно сравнить с перепиской через обычную почту, где конверт выполняет функцию инкапсуляции сообщения.

С помощью VPN удалось создать геораспределенную сеть, включающую VPN-каналы от конечных узлов (банкоматов, POS-терминалов в магазинах, удаленных касс) до отделений, а от отделений – до центрального офиса банка.

Время облаков

В первой сети банка был всего один сервер, стоявший под столом ИТ-директора. Вспоминаются айтишные байки про главную угрозу информационной системе – уборщицу со шваброй. И действительно, однажды уборщица вывела у нас банковскую сеть из строя. Потом к файловому серверу добавились сервер баз данных, сервер приложений, почтовый и веб-серверы. Потом выделили серверы под AD, DNS и DHCP. И все это приходилось дублировать для резервирования. Число серверов росло, под них отвели специальную комнату – серверную. Для экономии скачали дистрибутив VMware и начали использовать виртуализацию серверов. В итоге столкнулись с проблемами эксплуатации – в жаркое лето серверная перегревалась, основные серверы отключались вместе с резервными, и информационная система «падала».

Не добавляли оптимизма периодически появлявшиеся проблемы с электропитанием – то конфликт собственников, то обрыв кабеля, то плановые отключения электросети. Все это стимулировало перенос ИТ-инфраструктуры в дата-центры, специализирующиеся на услугах colocation, а затем и в развернутые в этих ЦОДах облака. Наступило время облаков, но об этом уже в следующей статье. ИКС

EKF – новый игрок на рынке телеком-оборудования для ЦОДов

Российский вендор электротехнических решений EKF выходит на рынок оборудования для дата-центров. На вопросы издания отвечает Сергей Хуторной, руководитель направления активного телекоммуникационного оборудования.

– EKF – известный российский производитель электротехнического оборудования. Почему бренд решил расширить линейку и выйти на рынок активного телекоммуникационного оборудования?

– Многие европейские и американские производители официально прекратили работу в России. Образовался вакуум, который надо было заполнить. 80% производственных мощностей EKF по-прежнему сфокусированы на производстве электротехнической продукции. Но два года назад мы начали развивать решения автоматизации и выпустили на рынок широкую линейку, включающую промышленные программируемые контроллеры, модули ввода-вывода с встроенными стандартными интерфейсами для подключения к периферийным устройствам (датчики, частотники, панели оператора) и системам контроля (OPC, SCADA), панели оператора, программируемые реле, контроллеры удаленного управления.

Развитие решений для телекома идет по нескольким направлениям. Первое – бытовой интернет вещей. Второе – промышленный IoT, включающий облачную платформу EKF Connect Industry, уже внедренную в эксплуатацию на ряде предприятий, в том числе на заводах EKF. Третье направление – промышленный Ethernet: от простых неуправляемых коммутаторов до управляемых на уровне L3, в промышленном исполнении для монтажа в шкафы управления. До конца года планируется выпуск многопортовых коммутаторов в стоечном исполнении для дата-центров.

– Что интересного EKF предлагает дата-центрам?

– В состав новой линейки активного телекоммуникационного оборудования EKF входят медиаконвертеры, преобразователи интерфейсов, SFP-трансиверы, промышленные коммутаторы, в том числе с поддержкой стандарта PoE. Промышленные PoE-коммутаторы обеспечивают подключение до 24 внешних устройств с потребляемой мощностью 36 Вт на канал. Среди таких устройств – поворотные видеокамеры, беспроводные устройства и другое полевое оборудование, которое может быть использовано для контроля и мониторинга как внутри дата-центров, так и на прилегающих территориях.

Промышленные коммутаторы EKF имеют высокую степень защиты от электромагнитных помех и скачков напряжения, поддерживают надежную связь в экстремальных условиях эксплуатации в диапазоне температур от −40 до +75°C. Линейка SFP-трансиверов производства EKF дает инженерам неограниченный выбор типа оптического волокна.

Активное телеком-оборудование EKF может быть использовано в инфраструктуре ЦОДа, в системах мониторинга окружающей среды и системах управления энергообеспечением. Кроме этого, EKF уже больше года выпускает пассивное оборудование для дата-центров под брендом TERACOM: СКС, шкафы, PDU, патч-корды, системы климат-контроля.

В настоящее время для СКС предлагаются решения «на меди», до конца года появятся высокоплотные оптические решения.

– Как быстро выполняются поставки? Как осуществляется поддержка?

– Если с нашего завода, то в течение недели в любую точку страны. Если нужно везти комплектующие из-за рубежа – до 45 дней.

Проблем с оперативной заменой вышедшего из строя оборудования не возникает – склады находятся в нескольких регионах России, в том числе в Новосибирске, Екатеринбурге и Краснодаре.

EKF использует дистрибьюторскую сеть продаж. Есть онлайн- и офлайн-программы обучения для партнеров и заказчиков. Проводится сертификация сотрудников партнеров, подтверждающая уровень их подготовки.

– Какие у EKF конкурентные преимущества на рынке дата-центров?

– EKF – надежный российский производитель, более 20 лет присутствующий на отечественном рынке. Штат насчитывает более 2000 человек, полсотни сотрудников занимаются R&D, обеспечивая постоянное технологическое развитие решений и проектирование нового оборудования. Бренд имеет производственные мощности в городе Александрове и поселке Ставрово Владимирской области и тщательно контролирует выпуск продукции на площадках партнеров, отвечая за качество вне зависимости от места производства.

Главное конкурентное преимущество на рынке – возможность предоставления комплексных решений, объединяющих продукцию для разных сегментов: промышленной автоматизации, телекома и инженерной инфраструктуры дата-центров. За счет многопрофильных инженерных компетенций и собственных производств продукция EKF соответствует самым высоким требованиям ЦОДов.

Энергоцентры высокой плотности для ЦОДов

Если при развертывании дата-центра требуется сэкономить площадь и время, то prefab-энергомодули высокой плотности – лучший выбор, убежден Михаил Саликов, директор по развитию компании «Хайтед».

– Компания «Хайтед» хорошо известна своей экспертизой в области строительства энергоцентров. Вы вывели на рынок контейнерные энергомодули высокой заводской готовности и высокой энергетической плотности. Почему занялись высокоплотными энергоцентрами и что подразумевается под этим термином?

– Заказчики из отрасли ЦОДов часто сталкиваются с дефицитом площади на своих объектах. Один из вариантов решения проблемы – использование энергоцентров высокой плотности, когда на ограниченном участке размещается многоуровневая система из специально подготовленных контейнерных энергомодулей, обеспечивающая повышенную электрическую мощность на единицу площади.

Если наш обычный предсобранный комплектный энергомодуль (prefab-энергомодуль) 1200 кВА обеспечивает мощность 43 кВт/кв. м, то двухэтажный энергоцентр из двух модулей – до 86 кВт/кв. м, а трехэтажный из трех модулей – до 129 кВт/кв. м. Причем это не просто конструкция из поставленных друг на друга обычных контейнеров, а гасящая влияние взаимных вибраций интегрированная система, обеспечивающая возможность работы prefab-энергомодулей в многоуровневом размещении.

– В чем преимущества использования энергомодулей «Хайтед» для ЦОДов?

– Прежде всего это экономия места в здании дата-центра. На одном из объектов при строительстве «по классике» потребовалось бы занять 84 кв. м, но использование нашего высокоплотного решения уменьшило площадь до 39 кв. м. Далее – быстрота развертывания на площадке. Мы поставляем уже готовое скомплектованное решение, выдающее требуемую заказчику мощность.

Кроме того, практика показывает, что сборка на объекте часто сказывается на качестве, поскольку работы выполняют разные подрядчики – кабельные линии прокладывают одни, щитовую сборку делают другие, автоматический ввод резерва (АВР) устанавливают третьи. Возникают нестыковки. «Хайтед» же предлагает полностью собранное и протестированное решение. Причем с общей гарантией, а не на отдельные устройства.

Еще одно преимущество – по желанию заказчика энергоцентр можно оформить или как капитальное строение, или как временное сооружение, что помогает оптимизировать финансовую нагрузку.

– Покупка prefab-решения для ЦОДов у мировых лидеров, как правило, обходится значительно дороже сборки на объекте. А у вас?

– Мы проводили расчеты для нескольких объектов. С учетом строительных работ наши prefab-решения получаются дешевле классического строительства на месте, особенно в случае гринфилд-проектов. Экспертиза и знание рынка позволяют выбрать оборудование, оптимальное по соотношению цена – качество. Кроме того, значительная часть стоимости решения у мировых лидеров приходится на бренд, а мы за имя денег не берем, хотя наш бренд хорошо узнаваем на рынке.

При этом следует отметить, что энергоцентр высокой плотности – это более сложное с инженерной точки зрения решение, чем отдельный prefab-энергомодуль, поскольку нужно обеспечивать защиту от повышенных вибраций. Требуется специальная подготовка оболочек, использование дополнительных элементов виброгашения. Если у заказчика большой участок, где можно разместить одноэтажные контейнеры, то дешевле обойдутся и сами контейнеры, и работы по их установке и обслуживанию.

– Что входит в состав prefab-энергомодуля для ЦОДов? Каков диапазон поставляемой энергомощности? Какие стандартные конфигурации предлагает «Хайтед»?

– Разработано несколько вариантов конфигураций. Базовый включает источники бесперебойного питания (модульные ИБП с АКБ), главный распределительный щит, прецизионные кондиционеры, систему локального и удаленного мониторинга.

В зависимости от пожеланий заказчика в состав могут входить АВР, переключающий потребителей с основной линии на резервную, система пожаротушения, пожарно-охранная сигнализация и ДГУ. Внутри модуля на площадке не требуется дополнительных монтажных работ – только подключение внешних линий.

– При каких температурах могут работать prefab-энергомодули «Хайтед»? Можно ли их использовать в районах Крайнего Севера?

– Диапазон рабочих температур – от −45 до +50°С. Использование термоизолированных контейнеров позволяет эксплуатировать модули и при −50°С. Более того, мы уже поставляли свои системы в районы Крайнего Севера на буровые установки. Так что на практике ограничения есть только для высоких температур – со стороны систем охлаждения.

– Каковы требования к площадке?

– Мы устанавливали энергомодули как на подготовленные монолитные

фундаменты, так и на временные плитные, причем даже в случае трехэтажного размещения. Конкретный выбор определяется состоянием грунта. Площадь для размещения энергомодуля 1600 кВА – 28 кв. м.

– Как обеспечивается мониторинг и диспетчеризация систем?

– Службы эксплуатации могут, не заходя в контейнер, контролировать состояние всех элементов энергомодуля: ИБП, кондиционеров, ДГУ. Используется наша система мониторинга Redpine, которая выводит информацию в облако «Хайтед» и на локальную SCADA ЦОДа. Под заказ может быть развернуто видеонаблюдение.

– Не возникают ли дополнительные проблемы у специалистов по эксплуатации при обслуживании многоэтажных конструкций?

– В энергомодулях для обслуживания предусмотрены специальные площадки, которые позволяют обходиться без подъемных механизмов. Основные сложности возникают при пусконаладочных работах, когда «Хайтед» использует подъемник. Замена батарей происходит максимум раз в пять лет, но и эту работу заказчик может переложить на нас в рамках сервисного обслуживания.

Конечно, службе эксплуатации с одноэтажными конструкциями работать удобнее – не надо ходить по лестницам. Но серьезных проблем нет, и если требуется сэкономить площадь, то энергоцентры высокой плотности – лучший выбор.

– Как решаете проблему поставки комплектующих после ухода с рынка мировых лидеров?

– Мы стараемся использовать продукцию российских производителей, проверенных партнеров. Но если заказчик запрашивает определенные импортные компоненты, то делаем кастомизированное решение. Существует проблема с импортозамещением ДГУ – их покупаем в Китае. Но обвязка ДГУ инженерными системами осуществляется в России. Как поставщик решения мы обеспечиваем полную гарантию независимо от используемых комплектующих.

– В чем конкурентные преимущества решений «Хайтед»?

– У «Хайтед» двадцатилетний опыт производства сложных решений, более трех лет – энергоцентров высокой

плотности. Продукты совершенствуют квалифицированные инженеры и специалисты отдела R&D компании, в том числе инженеры-проектировщики и сервисные инженеры ушедших с российского рынка западных компаний, обогатившие экспертизу «Хайтед» за счет опыта, который они получили за время работы у мировых лидеров.

Кроме того, у «Хайтед» свой штат разработчиков систем мониторинга и диспетчеризации, работающих над полностью российским, включая контроллеры и датчики, решением. В энергомодулях и в облаке используется созданное специалистами компании программное обеспечение.

Работаем быстро. У одного из клиентов от момента заключения контракта до поставки первого оборудования на площадку прошло полтора месяца.

– Как транспортируются prefab-энергомодули от завода до ЦОДа?

– Энергомодули поставляются в стандартных контейнерах, которые не предъявляют дополнительных требований при транспортировке. Используем автомобильный и железнодорожный транспорт. Возможна транспортировка модулей в удаленные районы вертолетом, но пока таких заказов не было.

При желании заказчик может перевозить энергомодули самостоятельно. Все зависит от контракта.

– Как обеспечивается гарантийное и постгарантийное обслуживание? Как проводится обучение персонала заказчика?

– У нас есть сервисная служба. Все обращения идут на первую линию поддержки. При необходимости на объект выезжает группа сервисных инженеров, которые выполняют гарантийное и сервисное обслуживание.

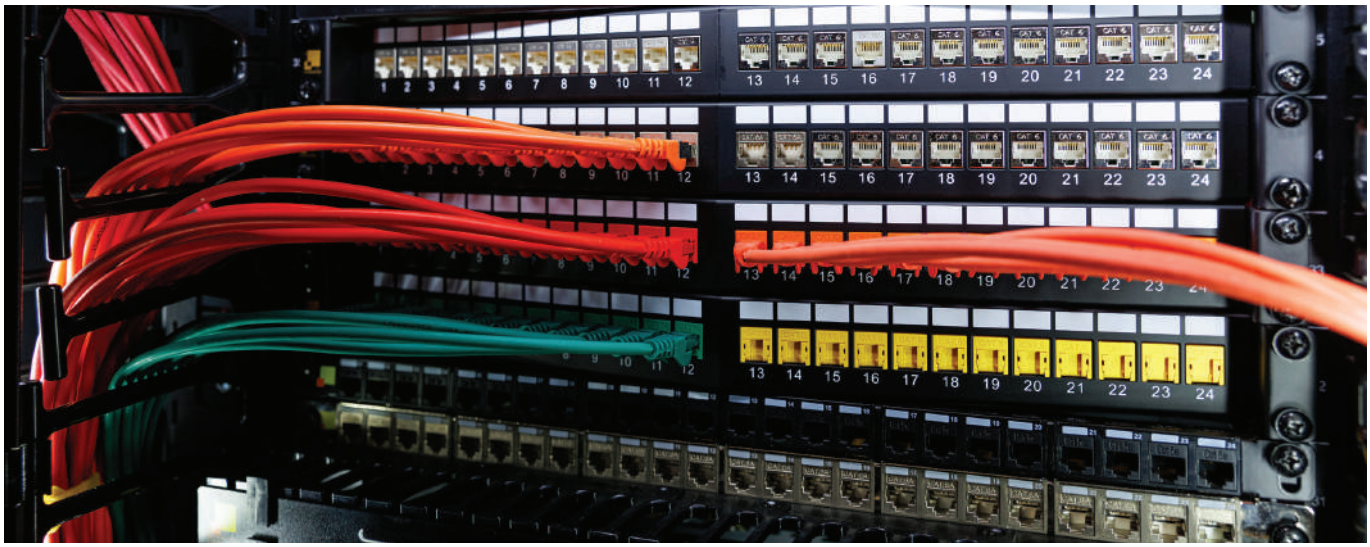
Наши штатные инженеры есть во многих регионах России (Новосибирск, Самара, Екатеринбург), а также в Алматы. Контракты заключаются на гарантийное и постгарантийное обслуживание, в том числе с SLA.

Базовое обучение персонала эксплуатации происходит на месте. Углубленное – в нашем учебном центре в Москве. По завершении обучения специалисту выдается свидетельство о том, что он прослушал курс и может эксплуатировать высокоплотные энергомодули.

– Можете ли назвать проекты внедрения энергоцентров высокой плотности от «Хайтед» в ЦОДах? Осуществляются ли поставки за рубеж?

– Например, наш энергоцентр установлен в ЦОДе, построенном PNK Group и недавно получившем сертификат уровня Tier III Uptime Institute. У нас есть проекты на территории ЕАЭС, в том числе в Казахстане. Мы готовы поставлять продукцию в любую дружественную страну, если в ней можно организовать надежную сервисную поддержку.

Калибровка, поверка и точность сертификационных измерений в СКС



Екатерина Оганесян, независимый эксперт, автор и ведущий преподаватель курсов по СКС в Бауманском учебном центре «Специалист»

Нужно ли поверять сертификационные тестеры для структурированных кабельных систем? Или их нужно калибровать? Или и то и другое? Что вообще понимается под поверкой и калибровкой в сфере СКС и как эти процедуры влияют на точность измерений?

Специалисты, которые работают с типовыми средствами измерений – вольтметрами, токовыми клещами, термометрами, манометрами и прочими техническими средствами, предназначенными для измерения определенных величин и имеющими нормированные метрологические свойства, с ходу скажут: тестеры нужно поверять. Причем в аккредитованной метрологической лаборатории. И добавят, что поверка в РФ обязательна, в то время как калибровка добровольна.

Специалисты по медным и волоконно-оптическим кабельным системам, работающие с тестерами для сертификации СКС – проектировщики, монтажники, менеджеры проектов, ГИПы, – так же с ходу ответят: нужна калибровка. Либо заводская, либо выполненная в организации, уполномоченной производителем тестера. Без нее поставщик фирменной СКС не примет результаты измерений, не зарегистрирует установленную систему и не выдаст на нее гарантию. Такой подход используют не только зарубежные поставщики СКС, по факту ушедшие с российского рынка, но и компании, которые заняли освободившуюся нишу и позиционируют себя как отечественные бренды-импортозаместители – «АльфаТек», «Гиперлайн», ДКС, Eurolan, ITK, LANMASTER и другие.

Различия по сути

Требование к тестеру для сертификации СКС иметь актуальный срок калибровки технически обосновано, поскольку при калибровке не только определяются действительные значения метрологических характеристик и удостоверяется пригодность прибора для проведения измерений, но и при необходимости **выполняется точная настройка, юстировка прибора – приведение его в состояние, обеспечивающее правильное функционирование**. Когда на кону выдача гарантии на кабельную систему, в интересах и поставщика СКС, и компании-монтажника, и заказчика быть уверенными в том, что прибор «не врет».

Поверка же не ставит перед собой задачу привести прибор в состояние, обеспечивающее правильное функционирование. Она нацелена только на определение и, возможно, подтверждение **соответствия характеристик средства измерений установленным требованиям**. Со-

ответствует требованиям – выдается свидетельство о поверке. Не соответствует – не выдается. Никакая настройка при этом не проводится.

Процедура калибровки технически шире, чем поверка, и с этой точки зрения сертификат о калибровке должен быть более весомым документом, чем свидетельство о поверке. Однако по действующим нормам РФ это не так. Причиной тому соображения не только технического, но и организационного, и юридического характера.

По закону

Статья 13 «Поверка средств измерений» закона № 102-ФЗ «Об обеспечении единства измерений» (ред. от 11.06.2021) гласит:

1. Средства измерений, предназначенные для применения в сфере государственного регулирования обеспечения единства измерений, до ввода в эксплуатацию, а также после ремонта подлежат **первичной поверке**, а в процессе эксплуатации – **периодической поверке**. Применяющие средства измерений в сфере государственного регулирования обеспечения единства измерений юридические лица и индивидуальные предприниматели обязаны своевременно представлять эти средства измерений на поверку.

2. **Поверку средств измерений** осуществляют **аккредитованные** в соответствии с законодательством Российской Федерации об аккредитации в национальной системе аккредитации **на проведение поверки средств измерений** юридические лица и индивидуальные предприниматели.

3. Правительством Российской Федерации устанавливается **перечень средств измерений**, поверка которых осуществляется только аккредитованными в соответствии с законодательством Российской Федерации об аккредитации в национальной системе аккредитации государственными региональными центрами метрологии.

Статья 18 «Калибровка средств измерений» того же закона гласит:

1. Средства измерений, не предназначенные для применения в сфере государственного регулирования обеспечения единства измерений, могут **в добровольном порядке подвергаться калибровке**. Калибровка средств измерений выполняется с использованием эталонов единиц величин, прослеживаемых к государственным первичным эталонам соответствующих единиц величин, а при отсутствии соответствующих государственных первичных эталонов единиц величин – к национальным эталонам единиц величин иностранных государств.

2. Выполняющие **калибровку средств измерений** юридические лица и индивидуальные предприниматели **в добровольном порядке могут быть аккредитованы** в области обеспечения единства измерений.

▲ **Рис. 1. Подключение модулей прибора DTX-ELT друг к другу через адаптер для установки эталонного значения перед началом работы**

Поверка – исключительно отечественное понятие, в иностранных стандартах его нет. Корнями термин уходит в нормативные документы СССР, ГОСТ 8.513-84 «Государственная система обеспечения единства измерений. Поверка средств измерений. Организация и порядок проведения». Для технически простых средств, таких как вольтметры, термометры и т.п., есть смысл в том, чтобы порядок был единым для всей страны, поэтому целесообразно поручить проведение поверки аккредитованным метрологическим лабораториям и таким путем обеспечить единство измерений. Когда точность средств измерений и соответствие требованиям удостоверяется независимой лабораторией, это препятствует возможным злоупотреблениям и служит дополнительным фактором надежности.

По действующим нормам поверка средств измерений в РФ обязательна. Сертификационные тестеры для СКС внесены в Госреестр средств измерений РФ, а значит, на них распространяется это требование. Однако принятые порядок и процедуры поверки разрабатывались задолго до создания сертификационных приборов для СКС и заведомо не учитывают их особенности. Это весьма сложное оборудование, программно-аппаратный комплекс, а не технически простое средство. Могут ли отечественные метрологические лаборатории выполнить поверку для столь сложного и многофункционального оборудования, есть ли у них необходимое для этого оснащение?

◀ **Рис. 2. Адаптер для установки эталонного значения DTX-Reference Module с физическим интерфейсом, соответствующим измерительным портам приборов DTX**

На практике

Чтобы проверить, соответствует ли прибор требованиям, к его модулям нужно подключить эталонное устройство с заранее известными характеристиками и сопоставить их с выдаваемыми показаниями. Зарубежные изготовители называют такое устройство «артефакт» и применяют его при калибровке приборов в своих сервисных центрах. Артефакт имеет физический интерфейс подключения, соответствующий измерительным портам прибора, и позволяет соединить его модули напрямую, без адаптеров постоянной линии и канала. Схема подключения по сути такая же, как применялась в устаревшем семействе DTX-ELT компании Fluke Networks для установки пользователем эталона перед началом работы с прибором (рис. 1).

В отличие от адаптера для установки эталонного значения (рис. 2), который применяется самим пользователем в повседневной работе с прибором, лабораторный калибровочный артефакт требует более высокой точности изготовления и стабильности характеристик. С ним работает персонал сервисного центра конкретного производителя приборов, и на нем калибруются тестеры определенной модели, принадлежащие разным заказчикам, с периодичностью раз в год.

Артефакты не универсальны. Это не магазин эталонных мер и не типовой калибратор, применяемые для средств измерений силы тока, напряжения, сопротивления и тому подобных параметров независимо от изготовителя устройства. Артефакт совместим только с конкретной моделью сертификационного тестера конкретного производителя, и его нет в открытой продаже. Для работы с ним применяется специализированный софт, и это не то программное обеспечение, которое идет в комплекте с прибором для загрузки результатов измерений на ПК, и не прошивка самого прибора – это специализированные утилиты, которых нет в открытом доступе.

За рубежом калибровка – сфера ответственности производителя приборов. Она выполняется либо на заводе-изготовителе, либо на базе фирменного сервисного центра. Понятия поверки просто нет в странах, не имеющих тех нормативных документов, которые мы унаследовали от СССР. В нашей же стране есть понятия и калибровки, и поверки. Но при этом в независимых метрологических лабораториях нет ни артефактов, ни специализированного ПО для работы с ними.

Проводить калибровку такие лаборатории не могут (вдобавок их не уполномочили на это производители приборов). Но могут ли они выполнить поверку? На бумаге – да, и соответствующие свидетельства выдавались и выдаются. С технической же точки зрения – нет, поскольку для действительного удостоверения выдаваемых прибором результатов необходимо использовать такой же артефакт и такое же подключение, как для калибровки. Разница только в том, что при поверке софт сверяет показания прибора с заранее известными параметрами артефакта и на этом останавливается (совпали значения – выдаем свидетельство о поверке, не совпали – не выдаем), а при калибровке при необходимости запускается процедура юстировки измерительных схем прибора, чтобы привести их в должное состояние, после чего выдается сертификат о калибровке.

Что же на самом деле могут проверить независимые лаборатории, если у них нет ни артефактов, ни специализированного ПО? По сути, единственный путь, чтобы хоть как-то удостовериться в работоспособности прибора – выполнить установку эталона так же, как это делает пользователь перед началом работы (у современных моделей это выполняется с помощью адаптера постоянной линии и адаптера канала, как показано на рис. 3), после чего провести измерения на некоей собственноручно сделанной эталонной линии длиной несколько десятков метров. И, в лучшем случае, сопоставить показания прибора с показаниями какого-то другого тестера, желательно откалиброванного его производителем. Так или иначе, все упирается в калибровку.

Упоминавшийся ранее закон № 102-ФЗ «Об обеспечении единства измерений» оперирует

понятиями поверки и калибровки с точки зрения метрологов, которые никогда не работали с СКС и сертификационными тестерами. А что говорят стандарты, регламентирующие именно построение и тестирование кабельных систем?

По ГОСТу

В ГОСТ Р 53245-2008 «Информационные технологии. Системы кабельные структурированные. Монтаж основных узлов системы. Методы испытания» про поверку не говорится ни слова, и тому есть причина: этот документ не разрабатывался в нашей стране, а переводился с американских и международных стандартов, в которых понятия поверки нет в принципе. Зато есть представление о функционале, точности и особенностях применения сертификационных тестеров. А значит, есть и требование калибровки – в нашем ГОСТ Р это пункт 3.1.4.3 «Заводская калибровка полевого тестера»:

- Полевой тестер, используемый для проведения испытания СКС, следует **регулярно калибровать на предприятии-изготовителе или в уполномоченном производителем агентстве** на соответствие спецификациям своих рабочих характеристик.
- Результаты испытания, полученные с помощью полевого тестера с просроченным калибровочным сертификатом, являются недействительными и могут быть не приняты при регистрации системы на предоставление гарантии.

В ГОСТ Р 53245-2008 также предусмотрены меры, позволяющие отследить износ адаптеров, чтобы их можно было вовремя заменить:

- Монтажникам СКС рекомендуется периодически проверять достоверность результатов измерений полевого тестера на эталонной линии (см. 3.1.4.6) для своевременного обнаружения таких отрицательных явлений, как механическое старение коннекторов и кабелей тестовых адаптеров и отклонение параметров полевого тестера от номинальных значений.

В пункте 3.1.4.4 «Проверка достоверности результатов измерений» описывается, как пользователю судить о состоянии и точности показаний прибора. Эти положения ГОСТ Р 53245-2008 скалькированы с американского стандарта TIA/EIA-568-B.2 от 2001 г. и не очень удачно переведены, поэтому в квадратных скобках даются уточнения автора по терминологии.

- Изготовитель полевого тестера должен предусмотреть возможность использования оператором простой процедуры для проверки достоверности

◀ Рис. 3. Установка эталонного значения в приборах AEM TestPro CV100 при помощи адаптеров постоянной линии и канала

результатов измерений в полевых условиях. Для такой проверки существует два вида процедур:

→ Воспроизводимость результатов измерений на эталонной линии [*правильнее было бы сказать «повторяемость» – в англоязычном источнике говорится «Repeatability of tests on a reference link»*]
Пользователю тестера рекомендуется собрать эталонную кабельную линию. Результаты последовательно выполняемых измерений на этой линии должны быть в пределах точности измерений, заданных для данного тестера. Все сравнения должны выполняться на основе «наихудшего случая» во всем диапазоне частот.

→ Стабильность результатов измерений, выполняемых в двух направлениях [*правильнее было бы сказать «сходимость» или «воспроизводимость» – в англоязычном источнике сказано «Consistency of tests by testing the same link in opposite directions»*]
Любая кабельная линия может быть протестирована сначала посредством присоединения управляющего модуля тестера к одному концу линии, а исполнительного модуля – к другому концу линии.
После выполнения теста управляющий и исполнительный модули меняют местами. Все результаты «наихудших случаев», полученные таким образом, должны быть в пределах диапазона точности измерений конкретного параметра, умноженного на 1,4.

По инструкциям поставщиков СКС

О применении эталонной линии, собранной пользователем, для отслеживания состояния прибора говорят и правила постановки объектов на гарантию, задаваемые поставщиками СКС. Формулировки у разных изготовителей если и различаются, то незначительно. Так, у одного из зарубежных поставщиков, чью гарантийную программу буквально скопировали многие отечественные бренды, в учебном руководстве приводились следующие положения:

Заводская калибровка

Все полевые тестеры должны проходить калибровку у изготовителя, в соответствии с его

требованиями и процедурами. Дата и время калибровки должны отображаться в программном обеспечении прибора и фигурировать в результатах тестирования.

Примечание 1: Подтверждение калибровки полевых тестеров в соответствии с заводскими требованиями (калибровочный сертификат) должно предоставляться в компанию – поставщика СКС по запросу.

Примечание 2: Компаниям-подрядчикам рекомендуется иметь эталонную линию для проверки повторяемости результатов измерений тестера. Адаптеры приборов для подключения к линиям и каналам со временем изнашиваются, поэтому следует время от времени проверять точность измерений на эталонной линии.

Упомянутые источники исповедуют непротиворечивый подход к сертификации СКС и калибровке измерительного оборудования. К сожалению, в более позднем ГОСТ Р 58749-2019 «Слаботочные системы. Кабельные системы. Тестирование кабельной системы. Основные положения» появились противоречия, которые усложнили ситуацию. Раздел 5.4 «Приборы для тестирования» гласит:

5.4.1 Сертифицированные кабельные анализаторы (тестеры)

Тестирование рабочих характеристик кабельных систем допускается проводить любыми приборами, которые предназначены для этого, исправны и поверены. Приборы должны иметь актуальные свидетельство государственного реестра средств измерений и свидетельство о поверке уполномоченной организации.

5.4.3 Заводская калибровка

Сертифицированный тестер, используемый для тестирования кабельной системы, должен регулярно проходить калибровку на предприятии-изготовителе или в уполномоченном производителем агентстве на соответствие спецификациям своих рабочих характеристик.

Копию актуального калибровочного сертификата необходимо прилагать к результатам тестирования. Результаты тестирования, полученные с помощью полевого тестера с просроченным калибровочным сертификатом, являются недействительными.

К ГОСТ Р 58749-2019 и его разработчикам возникают вопросы. Во-первых, о каком «сертифицированном тестере» идет речь? Кем он сертифицирован? Для чего? На самом деле речь идет

Принципиальные различия калибровки, поверки и установки эталонного значения ▼

Калибровка (Calibration)	**Определение фактических метрологических характеристик прибора и приведение его в состояние, обеспечивающее правильное функционирование** • Выполняется изготовителем тестера или уполномоченным сервисным центром • Срок действия 1 год. Дата и срок действия калибровки отображаются в прошивке прибора и могут изменяться только изготовителем или уполномоченным сервисным центром • Фигурирует в международных стандартах на СКС. Их требования создавались с учетом особенностей сертификационных тестеров. Периодичность, условия и выполнение калибровкци отводятся на усмотрение изготовителей приборов • Обязательное требование по отечественному стандарту ГОСТ Р 53245-2008, а также ГОСТ Р 58749-2019 • Выполняется добровольно согласно закону № 102-ФЗ «Об обеспечении единства измерений», ст. 18 • Обязательное требование зарубежных и отечественных поставщиков СКС для постановки установленной кабельной системы на гарантию – в противном случае результаты измерений не будут приняты к рассмотрению
Поверка	**Определение и, возможно, подтверждение соответствия характеристик средства измерений установленным требованиям. Не предусматривает выполнения юстировки и приведения прибора в состояние, обеспечивающее правильное функционирование** • Понятие отсутствует в зарубежных стандартах и нормативах • Обязательное требование согласно закону № 102-ФЗ «Об обеспечении единства измерений», ст. 13, и отечественному стандарту ГОСТ Р 58749-2019 • Изначальная цель – обеспечение единства измерений благодаря независимому подтверждению характеристик и точности приборов аккредитованными метрологическими лабораториями • Для действительной поверки сертификационных тестеров СКС требуется оснащение, которого у независимых лабораторий сейчас нет • Дата и срок действия поверки никак не отображаются в прошивке прибора • При наличии сертификата о калибровке требование о поверке избыточно и не имеет технического обоснования
Установка эталонного значения (Set Reference)	**Согласование работы модулей прибора между собой перед началом измерений** • Стандартами не регламентируется. Процедура описана в инструкциях производителей приборов • Выполняется пользователями самостоятельно, никакими сертификатами не оформляется • Проводится как для медной среды, так и для волоконной оптики. Для медных сред увеличивает точность измерения вносимых потерь, омического сопротивления и др. В оптических средах устанавливает уровень, относительно которого измеряются оптические потери в целевом сегменте (метод одной эталонной перемычки, иные методы) • Рекомендуется к выполнению перед каждым рабочим днем. Обязательно выполняется, если основной и удаленный модули впервые работают совместно; если модули подвергались перепаду температур; если имела место глубокая разрядка аккумуляторных батарей; если обновлялась прошивка прибора • Предотвращает использование для измерений чрезмерно изношенных адаптеров постоянной линии/канала, оптических эталонных тестовых шнуров

о **сертификационном** тестере – приборе, предназначенном для сертификации СКС. Во-вторых, какой смысл в том, чтобы требовать и поверку, и калибровку одновременно? Если выполнена калибровка, то требование поверки технически избыточно. Такой бюрократизм никак не повышает точность измерений. Если же учесть, что для действительной поверки необходимо по сути то же оборудование и ПО, что и для калибровки (а их по факту у независимых лабораторий нет), то это бюрократизм вдвойне. Вместо того, чтобы в стандарте отразить технически оправданный способ обеспечить точность измерений, пользователей вынуждают тратить немало времени и денег на лишние процедуры.

Что делать?

Правильнее было бы оснастить независимые лаборатории всем необходимым, чтобы они могли выполнять полноценную калибровку для различных моделей сертификационных тестеров. Это потребовало бы заключения договоров с разными производителями и соответствующих финансовых вложений, но тогда бы и средства, получаемые от калибровки, шли в бюджет метрологических лабораторий, и на практике выполнялся изначально разумный посыл обеспечивать единство измерений силами независимой стороны. Если юстировка не требуется, выдается свидетельство о поверке. Если потребовалось откалибровать прибор – сертификат о калибровке. Либо одно, либо другое.

Если же калибровка, как сейчас, остается в ведении производителей тестеров или уполномоченных ими сервисных центров, а независимые метрологические лаборатории не получают должного оснащения, тогда поверка – это профанация. В таком случае разумнее выделить сертификационные тестеры в категорию специализированных средств измерения, на которые не распространяется требование об обязательной поверке, раз независимые лаборатории все равно не могут ее полноценно провести. Требования о калибровке, изложенные в ГОСТ Р 53245-2008, необходимы и достаточны для того, чтобы на деле, а не декларативно, обеспечивать точность измерений.

Нюансы такого положения дел должны осознавать не только отраслевые эксперты и специалисты-метрологи, но и монтажники СКС, а также заказчики, которым устанавливают кабельные системы. Точность и достоверность измерений зависят от того, насколько грамотно пользователи сертификационных тестеров их эксплуатируют.

Описанная ранее эталонная линия и показанная на рис. 3 конфигурация для установки эталонного значения применяются самим пользователем в ходе эксплуатации прибора, но задачи у них разные. Первая задействуется время от времени – например, раз в квартал или когда получаемые значения стали вызывать сомнение. Сопоставление с ранее сохраненными параметрами эталонной линии позволит обнаружить, что результаты измерений «поплыли», и тогда следует либо заменить изношенные адаптеры, либо, если это не помогло, отдать прибор на калибровку или в ремонт. Установку же эталонного значения рекомендуется производить ежедневно перед началом работы. Эта процедура предназначена для согласования модулей прибора между собой – самопроверки его систем, сверки версий прошивки, выставления шкалы для замеров омического сопротивления и вносимых потерь. Но ни та, ни другая конфигурация не предназначены для использования в ходе калибровки или поверки, поскольку в них задействованы адаптеры постоянной линии и/или канала.

Современные адаптеры постоянной линии и канала имеют большой ресурс – несколько тысяч измерений. Однако в процессе работы с прибором они неизбежно изнашиваются, это расходные компоненты. При крайней степени износа прибор сам откажется использовать адаптеры для измерений и потребует провести замену. Но что, если степень износа не крайняя? Если в ходе поверочных процедур задействовать частично изношенные адаптеры, то как потом судить о точности получаемых результатов? Это существенный фактор неопределенности, и метрологическим лабораториям ни в коем случае не следует использовать такой подход.

Поверка и калибровка должны проводиться с минимумом неопределенности – только с собственными измерительными схемами прибора, без промежуточных звеньев в виде адаптеров постоянной линии и канала. А значит, без заводских артефактов и специализированного софта не обойтись. Остается надеяться, что Федеральное агентство по техническому регулированию и метрологии примет во внимание особенности работы с сертификационными тестерами для СКС и устранит существующие технические несоответствия. Противоречивые положения ГОСТ Р 58749-2019 необходимо исправить в любом случае – одновременные требования о поверке и калибровке избыточны. Остальное же зависит от договоренностей с изготовителями и возможности оснастить метрологические лаборатории всем необходимым для правильного выполнения процедур с сертификационными приборами для СКС. ИКС

Правильнее было бы оснастить независимые лаборатории всем необходимым, чтобы они могли выполнять полноценную калибровку для различных моделей сертификационных тестеров

Чиллеры Dunham-Bush для российских ЦОДов

Чиллеры высокой производительности – один из наиболее востребованных и дефицитных продуктов на российском рынке цодостроения. О преимуществах решений Dunham-Bush рассказывает Денис Белоусов, генеральный директор компании TermoIndustry.

– Когда и с какими решениями компания TermoIndustry вышла на рынок ЦОДов?

– Три-четыре года назад мы сделали первую попытку начать работу на рынке ЦОДов. Но, скажу честно, усилия наши были не слишком энергичными и не принесли особого результата. За прошедшее время компания выросла, стала более заметна на рынке систем охлаждения, и вот год-полтора назад мы увидели, что цодостроители сами начали проявлять интерес к предлагаемым нами решениям. Связано это не только с тем, что мы нарастили свою экспертизу и возможности, но и с увеличившимися масштабами проектов ЦОДов – ведь мы специализируемся именно на мощных системах холодоснабжения. Масштабы текущих проектов, в том числе на десятки мегаватт, позволяют максимально эффективно использовать решения тех вендоров, оборудование которых мы представляем в России.

– Получается, что рынок дорос до ваших масштабов?

– Можно сказать и так (*улыбается*). Вообще TermoIndustry – компания молодая, нам пять лет, но основана она профессионалами с серьезным опытом. Мы занимаемся в основном водоохлаждающими машинами, чиллерами. Причем ставка изначально была сделана на глубокое погружение в специфику каждой задачи, тщательную проработку технических решений совместно с заказчиком. Это позволило нам без всякой внешней поддержки, в том числе финансовой, успешно развиваться.

Мы работаем с немногими вендорами. По каждому сегменту оборудования у нас один якорный производитель. По чиллерам это компания Dunham-Bush, по градирням – Hon-Ming, по теплообменным аппаратам «воздух – вода» (драйкулерам) – Henry.

– Наиболее интересен заказчикам, наверное, Dunham-Bush как один из мировых лидеров в разработке и производстве чиллеров.

– Да, это крупный глобальный производитель, основанный 130 лет назад в США. Штаб-квартира компании находится в Малайзии, а производственные площадки – в нескольких странах. Головное предприятие с мощной научно-исследовательской базой расположено в КНР (Циндао, провинция Шаньдун). Это завод полного цикла, от механообработки винтов для компрессоров до испытательного стенда, где готовая продукция тестируется перед отгрузкой потребителю. Подчеркну, что это не сборочное предприятие, как у многих других производителей, использующих ключевые компоненты сторонних поставщиков, а полный цикл, с собственной компонентной базой. Много патентованных технологий и решений, у которых нет аналогов на рынке.

Продукция Dunham-Bush имеет серьезные конкурентные преимущества с точки зрения надежности, энергоэффективности, функционала. А в сочетании с высокой квалификацией наших инженеров, которые проходят регулярное обучение у производителя, получаем отличные технические решения для российских заказчиков.

– Какие решения Dunham-Bush имеют наилучшие перспективы на российском рынке?

– Компания выпускает широкий модельный ряд чиллеров разной мощности – как с воздушным, так и с водяным охлаждением конденсатора. Наиболее востребованы российскими заказчиками из индустрии ЦОДов чиллеры производительностью в диапазоне 0,4–1,3 МВт. Здесь мы ориентируемся на оборудование мощностью до 1,2–1,3 МВт – оно имеет оптимальное соотношение характеристик самой холодильной машины и затрат на логистику.

Конечно, у Dunham-Bush есть и более мощные чиллеры (вплоть до 10-мегаваттных машин с водяным охлаждением конденсатора), но это уже решения для промышленных объектов, для холодоснабжения технологических процессов. Для ЦОДов машины такой производительности целесообразно применять только для очень больших объектов, чтобы обеспечить необходимый уровень резервирования.

Сейчас для одного из российских заказчиков прорабатываем хладоцентр из 20 чиллеров по 1,8 МВт с водяным охлаждением конденсатора. При такой производительности одной машины обеспечивается необходимый уровень резервирования. Кроме того, получается красиво реализовать фрикулинг с возможностью плавного перехода на режим естественного охлаждения.

– А что с менее мощными аппаратами?

– Чиллеры производительностью 300–400 кВт также востребованы. Причем заказчики этих машин тоже заинтересованы в высокой надежности, энергоэффективности и удобстве регулирования производительности. Но на таких мощностях привычные спиральные компрессоры не всегда могут это обеспечить. Поэтому производители переходят к технологически более сложным решениям. Один из вариантов – применение центробежных безмасляных компрессоров Danfoss Turbocor или их аналогов. Это решение отличается высокой энергоэффективностью, но есть нюанс: минимальная нагрузка, при которой такой компрессор будет работать стабильно, составляет около 50%. При низкой нагрузке компрессора ста-

Выгрузка двух чиллеров Dunham-Bush ACDSX155R-FCN3 CC 550 кВт с функцией фрикулинга (FC) 500 кВт

бильность работы чиллера может снижаться, машина может перейти в предаварийное состояние. Данную проблему производители чиллеров решают путем установки двух центробежных компрессоров по 50% требуемой производительности, что значительно удорожает систему.

Dunham-Bush предлагает другое решение. При участии наших инженеров был разработан чиллер на базе холодильной машины серии ACDSX со встроенным фрикулингом, с применением винтовых компрессоров с синхронным двигателем на постоянных магнитах. При работе этого чиллера в режиме максимальной нагрузки его холодильный коэффициент практически равен показателю решения с центробежным компрессором, но при этом он более стабилен в работе и имеет широкий диапазон регулирования нагрузки. По этим характеристикам чиллер превосходит решения с центробежным компрессором. Еще один немаловажный плюс – более низкая стоимость. На сегодня это уникальное решение на рынке.

Важно подчеркнуть, что система управления безмасляным центробежным компрессором на магнитных подшипниках сложнее, чем у винтового компрессора, и требует дополнительных затрат, в том числе во время эксплуатации.

– С оборудованием понятно, а какие услуги вы оказываете заказчикам на основных этапах проекта ЦОДа?

– Если мы входим в проект, когда техническое задание уже утверждено, то возможностей для маневра немного, но определенная оптимизация возможна. Если же подключаемся с нуля, то во взаимодействии с заказчиком прорабатываем различные варианты технических решений, подбираем оптимальный.

Убедить заказчика, что оборудование будет работать, как заявлено, всегда можно, организовав тестирование чиллеров в лабораториях на заводе-изготовителе. Моделируются проектные условия нагрузки на холодильную машину. В присутствии заказчика проводятся испытания во всех возможных режимах, показатели фиксируются и документируются.

Далее – шеф-монтаж и пусконаладка. Наши инженеры вооружены «до зубов» всем необходимым инструментарием, всесторонне обучены производителем и в кооперации со специалистами заказчика способны решить самые сложные задачи.

На этапе эксплуатации сервисное обслуживание могут осуществлять как наши инженеры, так и обученные специалисты службы эксплуатации заказчиков. Время реакции – основной критерий эффективности обслуживания, особенно для ЦОДов. Если это время должно быть малым, то рекомендуем заказчику обучить собственную службу эксплуатации, особенно на больших объектах, и разместить на площадке ЗИП, который формируется на этапе заказа основного оборудования и рассчитывается на год-два эксплуатации.

– Сейчас много разговоров о повышении мощности стоек из-за роста популярности приложений на базе искусственного интеллекта. Непосредственно с высокоплотными стойками связано прямое жидкостное охлаждение (DLC). Есть ли у вас соответствующие решения?

– Действительно, повышение энергетической плотности стоек и увеличение монтированной мощности ЦОДа требуют отведения большего количества тепла. Как я уже говорил, наша специализация – это охлаждение жидкости (теплоносителя). Предлагаемые нами решения – холодильные машины (чиллеры) и теплообменное оборудование – могут использоваться как для ЦОДов с воздушным охлаждением, когда воздух охлаждается жидкостью через теплообменник, так и для прямого жидкостного охлаждения. На мой взгляд, в России контактные системы DLC с охлаждающей пластиной (теплообменником) будут развиваться быстрее иммерсионных (погружных) систем.

– Как вы оцениваете перспективы использования оборудования Dunham-Bush в российских ЦОДах?

– С большим оптимизмом. Этот оптимизм основан на интересе со стороны заказчиков: они обращаются к нам все чаще. Значит, цодостроители по достоинству оценивают и технику Dunham-Bush, и экспертизу инженеров TermoIndustry. У нас уже есть положительный опыт инсталляции чиллеров Dunham-Bush большой производительности на коммерческих и промышленных объектах (в различных отраслях). Думаю, скоро мы сможем представить и первые цодовские проекты.

Прыжок в эру ИИ, или Пять вопросов к проекту «Экономика данных»

Николай Носов

Взаимодействие с бизнесом, предоставление открытых данных, требования к их качеству и безопасность – темы, раскрытие которых хотелось бы увидеть в документах нового нацпроекта.

Вопросы безопасности

Прошедший в Москве дата-саммит «Прыжок в эру ИИ» начался с красочного представления. Демонстрирующие «прыжок» акробаты на прикрепленных к ногам пружинах высоко взлетали и кувыркались в воздухе под потолком лофта Quattro Space. Красиво, молодежно, современно и... немного нервно. Особенно для сидящих в первом ряду, когда в метре от них с потолка, грозно размахивая механическими приспособлениями, падали серебристые спортсмены.

Не знаю, входило ли это в замысел организаторов, но шоу породило вопрос: насколько безопасным будет прыжок в эру ИИ. В памяти всплыли страшилки – от ставшего с появлением боевых дронов с ИИ реальностью Терминатора до полностью контролирующего поведение всех людей ИИ-бога из третьего сезона сериала «Мир Дикого Запада».

Среди ключевых тем мероприятия – подготовка данных для эффективной работы с искусственным интеллектом и обсуждение концепции национального проекта «Экономика данных». Перспективы нацпроекта, как можно было заключить из рассказа генерального директора DIS Group Павла Лихницкого, весьма радужные. Инвестиции в него до 2027 г. достигнут 1,6 трлн руб., а ожидаемый вклад в ВВП страны составит 11,2 трлн руб. П. Лихницкий привел также данные опроса Gartner, согласно которым к основным проблемам генеративного ИИ относятся качество данных (46% опрошенных) и вопросы безопасности (39%).

Для нашей страны вопросы информационной безопасности более чем актуальны. Причем не стоит забывать, что ИБ включает не только защиту персональных и критичных для функционирования экономики и обороноспособности страны данных, но и этику ИИ. Пока до конца не понятно, как эти вопросы будут решаться в рамках нового нацпроекта.

Качество данных

Искусственный интеллект без качественных данных неэффективен. Если обучать его на всем подряд из интернета, то получим скандалы, подобные случившему недавно, когда на вопрос, почему в мультфильме «Маша и Медведь» девочка живет одна, яндексовская Алиса ответила, что Маша – это призрак убитой девочки. Генеративный ИИ AI Overviews от Google пошел еще дальше: не поняв шутку в комментариях, предложил добавлять в соус для пиццы клей, а для борьбы с депрессией – спрыгнуть с моста «Золотые ворота».

Точность, достоверность и прозрачность обеспечивается в рамках систем управления данными. Ниши, возникшие на рынке после ухода зарубежных вендоров, успешно заполняют российские компании, недостаток компетенций восполняющие за счет кооперации и создания альянсов. Примером может служить подписание соглашения о стратегическом сотрудничестве «Ростелекома» и компании DIS Group, занявшей в мае 2024 г., по данным исследования ЦСР «Рынок систем управления и обработки данных», первое место по доле рынка (23%). Это серьезная заявка на успех в борьбе за контракты нацпроекта с основными конкурентами, среди которых Сбер. Вопрос в требованиях к обеспечению качества данных, которые будут предъявляться к участникам конкурсов.

> Считаю, что потребность в открытых данных есть. Рынку интересен синергический эффект от обезличенных данных, открытых данных о номенклатуре изделий, ГОСТах. В текущей парадигме это разрозненная информация. Предоставление открытых данных в рамках нацпроекта или государственного сервиса привело бы к повышению эффективности, ведь они участвуют в цепочках создания ценностей предприятий. Такие идеи обсуждаются, в том числе на уровне Гостеха. Вопрос – какие данные можно без ущерба сделать общедоступными.

Павел Лихницкий, генеральный директор DIS Group

Готовность бизнеса и общества

В отличие от традиционной экономики, где основной акцент делается на производстве и распределении материальных благ, экономика

Уровни зрелости управления данными

Источник: DIS Group

Иван Бегтин, директор и соучредитель некоммерческого партнерства «Информационная культура»

> Все данные, названные на сайтах госорганов открытыми, таковыми не являются, бесполезны или не обновлялись от четырех до восьми лет. Создать портал открытых данных без государства не столь сложно, сколь сложно его держать актуальным. Самые очевидные направления для перезапуска темы открытых данных в России – машиночитаемые нормативные документы, тексты для машинного обучения, систематизация и агрегация научных данных и много-много-много датасетов. Это недорого, но этим некому заниматься внутри государства, и не похоже, что кто-то появится в ближайшие годы.

данных базируется на обработке информации. Переход требует не только развертывания технических решений, но и зрелости в управлении данными, готовности общества и бизнеса использовать новые технологии, такие как машинное обучение и искусственный интеллект.

Готов ли российский бизнес к переходу на экономику данных? Обсуждение показало, что прогресс есть. Согласно представленному на дата-саммите исследованию DIS Group «Оценка зрелости управления данными», в период с 2018 по 2023 гг. доля компаний, которые находятся в процессе реализации инициатив по управлению данными, выросла с 17 до 89%.

Метрика «Бизнес-ценность» от управления данными увеличилась по сравнению с 2018 г. на 22%, что свидетельствует о растущем желании бизнеса получать выгоды и извлекать дополнительную ценность из имеющихся данных. Существенный рост, более 25% по сравнению с 2018 г., наблюдается по метрике «Компетенции», так что инвестиции компаний в развитие навыков и опыта сотрудников дают свои плоды. Радужно выглядят перспективы: согласно прогнозу DIS Group, к 2028 г. доля компаний, реализующих инициативы по управлению данными, приблизится к 98%.

Стоит отметить, что опрос проводился среди ведущих российских компаний, четверть которых – банки. Если бы опрашивались представители среднего и малого бизнеса, а также госслужащие, картина была бы не столь оптимистичной.

Открытые данные

Лет пять назад в стране активно обсуждались вопросы открытых данных (ОД) – свободно доступных, лицензионно чистых, машиночитаемых хранилищ первичных данных, в том числе государственных данных, собираемых госорганами при выполнении их функций. Преимущества очевидны: ОД повышают доверие к органам госвласти, создают условия для работы исследователей, предпринимателей и разработчиков новых сервисов, способствуют развитию технологий, включая разработку новых методов анализа данных и инструментов для их визуализации.

Первые шаги внушали оптимизм. Был создан федеральный портал открытых данных РФ (data.gov.ru), появились разделы с ОД на региональных порталах, в частности на портале Москвы.

Однако в последнее время интерес государства к этой теме снизился – региональные базы данных перестали обновлять, а федеральный портал уже год как не работает. «Многие не готовы открывать реально необходимые данные, а те, что открываются, как правило, бесполезны для отрасли. На портале открытых данных собрали много разных, но индустрия не нашла способов их использования», – пояснил вице-президент, директор по ИИ и управлению данными «Ростелекома» Сергей Носов.

Эксперт отметил, что в рамках проекта «Экономика данных» и развития ИИ видит большой запрос государства, в частности Минцифры, на создание платформы открытых данных, в рамках которой будет собираться именно то, что нужно бизнесу. Минцифры активно взаимодействует с отраслью, запрашивает, что интересно и для каких задач, прорабатывает логику обезличивания, шифрования и предоставления такого сервиса вовне. Есть планы до конца года создать такое решение в отдельной предметной области.

Некоторые эксперты рассматривают в качестве платформы ОД создаваемую Минцифры государственную информационную систему для организации работы с большими данными, в которую будут загружаться обезличенные датасеты. Но доступ в нее будет предоставляться не всем, а только авторизованным разработчикам. Есть опасение, что в их число не попадут независимые исследователи, небольшие компании и стартапы. Строго говоря, ОД эти дата-сеты считать нельзя. Так что вопрос, будет ли государство заниматься открытыми данными в новом нацпроекте, и если да, то как станет трактовать этот термин, остается пока без ответа.

Обещанного три года ждут

Но главный вопрос – когда будет сформулирован в окончательном виде проект «Экономика данных». Сначала анонсировалось, что проект запустят до конца 2023 г. В ноябре 2023 г. на стратегической сессии по формированию национального проекта «Экономика данных» заявлялось, что паспорт нацпроекта «Экономика данных» с конкретными показателями и результатами будет подготовлен к лету 2024 г. Лето началось, а документов пока нет.

Выполнение нацпроекта «Цифровая экономика» завершается в 2024 г. Так что для утверждения идущего ему на смену проекта «Экономика данных» времени осталось немного. ИКС

Пять принципов бесперебойной работы ИТ-инфраструктуры

Бесперебойная работа приложений – ключевое требование любого бизнеса и главный показатель качества облачного провайдера. Как в современных реалиях российского рынка обеспечить выполнение этого требования и на что смотреть при выборе облака – разбираемся вместе.

Олег Федоров, руководитель направления облачных продуктов и решений, Linx Cloud

Геораспределенность и «железо»

Базовое условие надежности информационных систем и ИТ-сервисов в облаках – развертывание необходимой ИТ-инфраструктуры на нескольких площадках с настроенным резервированием. Это обеспечивает стабильность работы приложений даже в случае аварий. Наличие нескольких зон доступности, т.е. дублирование приложений и сервисов в различных локациях – залог того, что система не «упадет» из-за проблем на одной площадке.

Соответственно, имеет смысл отдавать предпочтение провайдерам, обладающим сетью ЦОДов или как минимум несколькими площадками в разных регионах. Тогда появляется возможность создавать архитектуры с необходимой географической распределенностью.

При выборе гибридного формата локальные ресурсы компании объединяются с облачными площадками одного провайдера, скажем, в двух разных локациях. Также можно добавить собственное оборудование в ЦОДе другого провайдера (colocation) – и ИТ-система, построенная на подобной архитектуре, будет работать ощутимо надежнее.

Другая ключевая составляющая – оборудование, на котором развернуто облако. Экономика играет здесь важнейшую роль. Некоторые провайдеры могут сознательно выбирать более доступное оборудование, чтобы увеличить свою прибыль за счет маржи, и такое оборудование может быть менее надежным. Этот подход повышает риски частого и массового отказа серверов и СХД, что неминуемо скажется на бизнесе клиентов. Мелкие провайдеры более уязвимы, поскольку их инфраструктура не обладает масштабами, необходимыми для распределения рисков. Выход из строя даже нескольких узлов в их облаке может привести к значительной деградации ИТ-сервисов.

Разброс в стоимости оборудования огромный, особенно когда речь идет о системах хранения данных (СХД), поэтому в зависимости от архитектуры «падение» СХД может быть как незначительным инцидентом, так и катастрофическим, возможно, с необратимой потерей данных клиента.

Программно определяемые системы хранения данных (SDS) представляют собой одно из решений, призванных снизить зависимость от отдельных физических устройств. Но даже они не являются универсальным ответом: случаи сбоев open source SDS показывают, что восстановление работоспособности – это только часть задачи. Поте-

рянные в результате сбоя данные могут оказаться гораздо более серьезным вызовом, а их восстановление может затянуться на долгое время.

Найти оптимальную пропорцию рентабельности, маржинальности и надежности «железа» нелегко. Косвенным индикатором здесь может служить цена на услугу: если провайдер собрал свой парк из топовых линеек оборудования, то чаще всего ему будет трудно удерживать рыночный уровень цен, они будут заметно выше. И наоборот – излишняя ценовая доступность по сравнению с общерыночным уровнем может свидетельствовать о том, что на «железе» серьезно сэкономили.

Впрочем, ни тот ни другой вариант сами по себе не являются ни гарантией выдающегося качества сервисов, ни знаком того, что все будет работать плохо.

Не запутаться в сетях

Сетевая инфраструктура не менее важна. Сейчас, когда даже домашние роутеры предлагают скорость 10 Гбит/с, облачным провайдерам требуется гораздо бóльшая пропускная способность. Например, для 30 хостов в облаке скорости 10 Гбит/с может и хватить, но при кластере из 1500 хостов не обойтись без 100-гигабитных интерфейсов. Такая пропускная способность нужна для того, чтобы эффективно обрабатывать актуальные объемы трафика данных.

Выбирая между созданием собственного решения и покупкой готового, всегда имейте «план Б»

Важно также разделение сетей: если провайдер использует один и тот же физический интерфейс для передачи данных между виртуальными машинами и трафика СХД, то это может привести к коллапсу всей системы из-за перегрузки, вызванной всего лишь одной «забуксовавшей» виртуальной машиной. Для поддержания нужного уровня отказоустойчивости трафик нужно «разводить», но разделение сетей на сегменты (SAN и Ethernet, а также Infiniband) удваивает издержки.

Узнать о таких деталях организации сети можно только от самого провайдера, оценить их наличие по внешним признакам практически невозможно. Подобные вещи можно уточнить на предпродажном этапе, предложив в качестве пробного камня для ресурсов провайдера умозрительный пример, в котором важны все перечисленные моменты, связанные со скоростью передачи данных и распределением их потоков.

Командное усилие

Ключевой фактор успеха любого облачного провайдера – его команда. Наилучшее «железо» и передовые технологии окажутся бесполезными, если инженеры не имеют достаточной квалификации. Компетентность инженеров особенно важна, когда облако построено на таких решениях виртуализации, как OpenStack. В нем ответственность за поддержку и устранение неполадок не лежит на одном вендоре, и далеко не всегда есть четкие инструкции по устранению проблем.

Российские вендоры open source-решений виртуализации все еще находятся в стадии роста, поэтому у них, скорее всего, недостаточно ресурсов и опыта для устранения специфических проблем, которые могут возникнуть в конкретном ЦОДе. Значит, команда провайдера должна уметь самостоятельно справляться с трудностями, зачастую обходясь без каталога типичных ошибок и вопросов, что весьма непросто при наличии «детских болезней» у многих новых решений.

Если компания развивает облачную платформу на основе своего продукта, то присутствие в штате экспертов, которые непосредственно занимаются его разработкой и поддержкой, становится большим плюсом. В случае с готовыми продуктами оценить надежность облака позволяют только опыт эксплуатации и время.

Выбирая между созданием собственного решения и покупкой готового, всегда имейте «план Б». И помните, что даже неприметная «серая лошадка» на рынке может оказаться надежным выбором, если за ней стоит команда с необходимым опытом и ресурсами для поддержки.

ИБ-призма

В контексте информационной безопасности важно различать, какие сервисы компания использует для собственных нужд, а какие предлагает клиентам. Несоответствие между этими двумя аспектами может свидетельствовать о потенциальных уязвимостях в облачной инфраструктуре. Многие провайдеры стремятся настроить свою инфраструктуру согласно требованиям регуляторов, что позволяет обеспечить высокий уровень защиты, в том числе с помощью систем типа IPS, SIEM и SOC. В таком случае провайдер способен устранять ИБ-проблемы клиентов так же, как свои собственные, теми же ресурсами и с такой же эффективностью.

В современном ПО огромное внимание уделяется безопасности еще на этапе разработки, когда в облаке работают инструменты для анализа кода, выявляющие уязвимости приложений до выпуска новых версий. Они помогают обнаружить недочеты, которые могли быть пропущены или даже умышленно внедрены в код, что крайне важно в условиях постоянного повышения требований к безопасности приложений.

Cloud native

Один из главных факторов эффективной и безопасной эксплуатации информационных систем в облаке – адаптация ландшафта и

ИТ-сервисов к стандартам cloud native. Этот подход предполагает разработку приложений непосредственно для облачных сред, что обеспечивает их оптимальную работу, масштабируемость и управляемость на различных платформах.

В legacy-системах, перенесенных в облако без должной подготовки, часто возникают проблемы производительности и стабильности, так как исходно они не были «заточены» под такую эксплуатацию. Cloud native-приложения разрабатываются с учетом специфики облачной среды, что позволяет им максимально использовать ее возможности. Они основаны на микросервисной архитектуре, где приложение разделено на множество независимых сервисов, каждый из которых выполняет свою функцию.

Микросервисы упаковываются в контейнеры, обеспечивающие необходимую среду для их работы и упрощающие развертывание. Оркестрация контейнеров, например, с помощью инструмента Kubernetes, помогает управлять этими контейнерами, автоматизируя их развертывание и масштабирование. Разработка подразумевает использование облачных сервисов и ресурсов, а также применение практик непрерывной интеграции и доставки для ускорения выпуска обновлений.

Cloud native-приложения более гибкие, их легче масштабировать, благодаря чему можно калибровать и добавлять объемы СХД, вычислительные и сетевые ресурсы по мере необходимости. Это, в свою очередь, обеспечивает высокую устойчивость к сбоям, поскольку проблемы в одном компоненте не останавливают всю систему. А автоматизация процессов разработки и развертывания позволяет проводить обновления быстро и с минимальными рисками.

Экономия затрат достигается за счет оплаты только используемых ресурсов, а возможность быстро реагировать на запросы пользователей улучшает их опыт от эксплуатации продукта. Правильно подобранный API обеспечивает необходимую интеграцию и взаимодействие cloud native-сервисов вне зависимости от локации облака и его технической спецификации.

Поэтому оптимальной стратегией для бизнеса может стать изначальная ориентация всех новых элементов ИТ-ландшафта на подход cloud native – просто для того, чтобы избежать зависимости от инфраструктуры в будущем. Широкое предложение провайдерами PaaS-сервисов для разработки всего необходимого сразу в расчете на облако должно в этом помочь и является своего рода движением навстречу такому спросу. Платформенные решения сегодня разрабатывают и совершенствуют почти все ведущие игроки рынка.

Что касается совмещения cloud native- и legacy-ИТ, то один из наиболее очевидных способов заключается в постепенной модернизации старых приложений, включая их рефакторинг с целью оптимизировать для контейнеризации. Некоторые legacy-приложения проще и экономически выгоднее будет «упаковать» в контейнеры для запуска в облачной среде без переписывания исходного кода.

■■■

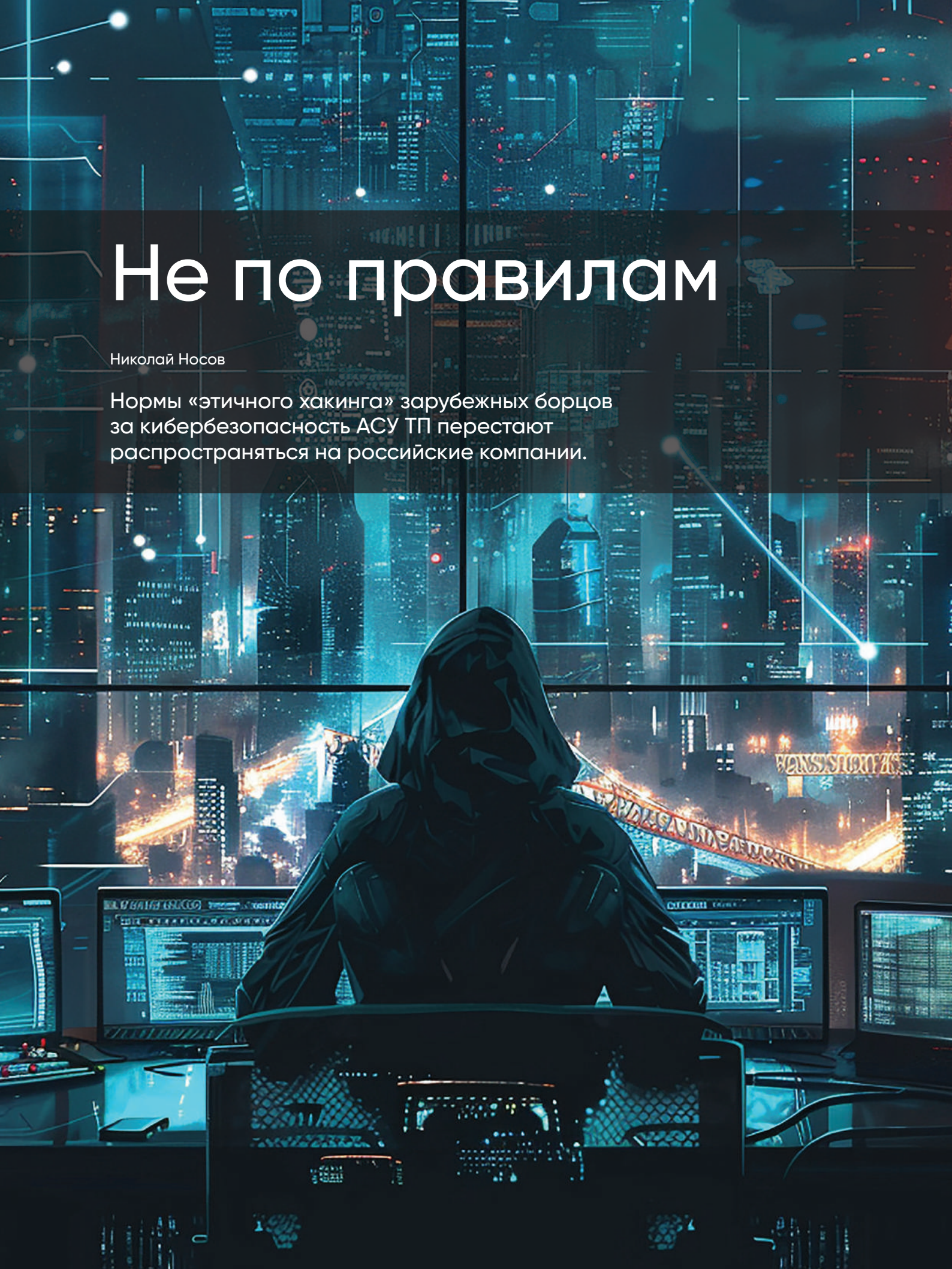
Для того чтобы эксплуатация и развитие ИТ-инфраструктуры представляли собой контролируемый бизнес-процесс, а не постоянный очаг напряженности, к проектированию архитектуры нужно подходить комплексно. Все требования к «железу», ПО, провайдерам, резервированию инфраструктуры и данных должны укладываться в единую стратегию, исходящую из того, насколько бизнес конкретной компании зависим от стабильности ее ИТ-систем. ИКС

Оптимальной стратегией для бизнеса может стать изначальная ориентация всех новых элементов ИТ-ландшафта на подход cloud native

Не по правилам

Николай Носов

Нормы «этичного хакинга» зарубежных борцов за кибербезопасность АСУ ТП перестают распространяться на российские компании.



Еще недавно в мире играли по простым правилам: есть легальный бизнес, стремящийся получить прибыль и минимизировать потери, и есть криминал, атакующий бизнес с целью получения денег. Конечно, бизнес нередко был «серым» и смешивался с криминалом, но во всем мире, по крайней мере на публичном уровне, такое смешение осуждали как нарушение правил, а страны сотрудничали в поимке преступников.

Правила распространялись и на компьютерные преступления, особенно такие, когда воздействие на компьютерную систему в виртуальном мире приводит к техническому инциденту в реальном. Когда воруют конфиденциальную информацию, это неприятно. Когда хакер через интернет переводит стрелки и пускает поезд под откос – смертельно.

Выявляли уязвимости компании по обеспечению информационной безопасности, искали удачу «белые хакеры», но железным правилом оставалось сначала оповестить вендора о найденной у него проблеме, дать время на латание дыр и лишь потом публично сообщать о находке. На это правило не влияли политические конфликты и войны. Атака на физическую инфраструктуру – вещь обоюдоострая. В киберпространстве нет границ: вынесенной в публичное поле уязвимостью может воспользоваться каждый, и неизвестно, по кому будет нанесен удар.

Не корысти ради

События 2022 г. перевернули картину. В соседней, некогда дружественной стране практически легализовали компьютерный криминал – не скрываясь, работают колл-центры, обманом крадущие деньги у российских пенсионеров, публикуются инструкции по проведению кибератак, поощряется создание армии преступников-любителей – хактивистов, нагружающих защитные системы российских предприятий.

Пошатнулось и правило не сообщать публично об уязвимости до информирования о ней вендора. Во всяком случае российского вендора. Старший исследователь угроз информационной безопасности «Лаборатории Касперского» Вячеслав Копейцев на прошедшей в Губкинском университете конференции RUSCADASEC CONF 2024 рассказал об опубликованной в марте 2023 г. статье Хосе Бертина, в которой автор без предупреждения описал эксплуатацию уязвимостей в решениях одного из российских производителей средств диспетчеризации инженерного оборудования. Хорошо, что статью заметили в «Лаборатории Касперского», незамедлительно связались с Национальным координационным центром по компьютерным инцидентам и компанией. В ходе расследования подразделение Kaspersky ICS CERT выявило 141 устройство российского вендора, доступное для атак через интернет. К счастью, до ликвидации уязвимостей никто ими воспользоваться не успел.

Атаки на цепочку поставок, т.е. на зачастую имеющих более слабые системы защиты подрядчиков уже стали обыденными. Новое – на сторону криминала переходят сами подрядчики. Например, NGFW, установленный на сети одной газопоршневой станции, зафиксировал значительные объемы трафика, исходящего из АСУ ТП предприятия. Расследование выявило вредоносную программу для проведения DDoS-атак на сервере SCADA. Затем был обнаружен канал удаленного доступа в технологическую сеть, который, как оказалось, остался у украинского подрядчика с 2019 г., когда велись пусконаладочные работы. Через канал подрядчик загрузил вредоносное ПО, используемое для проведения DDoS-атак на российские сайты.

Для лечения сервера требовалась перезагрузка, но этому воспротивились технологи, не желавшие допустить простоя сервиса. Тогда компания не нашла ничего лучшего, чем обратиться к украинскому подрядчику с просьбой сообщить пароль привилегированного доступа к системе (root). Реакция последовала уже через пять минут: подрядчик, вместо того чтобы сообщить пароль, удаленно подключился и начал менять уставки с целью вывести оборудование из строя. Спасло только экстренное отключение питания сервера.

Изменились и цели атак. Раньше целью были деньги, и если затраты на атаку не окупались, ее не проводили. Теперь цель – причинить максимальный ущерб и произвести пропагандистский эффект. Во многом поэтому так выросло число атак на АСУ ТП, которые в мирных условиях редко интересовали преступников из-за сложностей проникновения и дальнейшей монетизации.

Например, проукраинская хакерская группировка в пропагандистских целях разместила в Telegram-канале скриншоты, подтверждающие взлом системы управления нефтяными скважинами одной российской компании. Расследование показало, что система, управляющая скважинами через VPN-каналы, находилась на виртуальной машине в публичном облаке. Через интернет злоумышленникам удалось сделать SQL-инъекцию, т.е. внедрить вредоносный SQL-код в запрос к базе данных. Быстрое расследование и многоуровневая защита смогли предотвратить выход из строя оборудования, чего пытались добиться хакеры путем изменения уставок и перевода устройств в аварийный режим. Понятно, что никакой финансовой выгоды от этого они бы не получили.

Когда воруют конфиденциальную информацию, это неприятно. Когда хакер через интернет переводит стрелки и пускает поезд под откос – смертельно

▲ Рис. 1. Источники атак на АСУ ТП в 2023 г.

▲ Рис. 2. Приоритеты в кибербезопасности АСУ ТП у конечных пользователей в 2023 г.

Дать нельзя запретить

Цифровизация повышает эффективность бизнеса, но упрощает работу преступникам. По данным отчета «Тенденции развития киберинцидентов АСУ ТП», представленного экспертно-аналитическим центром InfoWatch, основной канал (37%) атак на АСУ ТП – это устройства, подключенные к интернету (рис. 1).

В итоге бизнес задумался о целесообразности внешних подключений. Если в 2021 г. к интернету были подключены более 70% устройств АСУ ТП, то в 2023 г. – меньше половины.

Ограниченность мониторинга и преодоление, как правило, лишь одного уровня защиты при взломе модема и подключенного к нему устройства делают привлекательными атаки на предприятия с распределенной инфраструктурой АСУ ТП: нефтегазового сектора, угольной и лесной промышленности, сельского хозяйства, коммунальных служб и транспорта. На средства удаленного доступа приходится 20% атак на АСУ ТП, и это необходимо учитывать при проектировании средств защиты.

Атака украинского подрядчика на газопоршневую станцию – наглядный пример необходимости контролировать внешние подключения и текущее состояние инфраструктуры. Своевременная актуализация данных и мониторинг систем АСУ ТП – отправная точка обеспечения безопасности. Это, по мнению 62% опрошенных InfoWatch специалистов по безопасности АСУ ТП, приоритетное направление защиты (рис. 2). Второе по важности направление (48%) – адекватная оценка рисков тех или иных решений.

Но очевидно, что правильнее озаботиться безопасностью АСУ ТП еще при проектировании. Ведь затраты на то, чтобы не допустить появления уязвимости, на порядки меньше, чем на то, чтобы ее устранить при обнаружении на этапе эксплуатации.

...Когда в начале десятых годов стали проводиться конференции по кибербезопасности АСУ ТП, многие специалисты относились к ним скептически. Зачем заниматься несуществующей проблемой? Ведь технологический контур не имеет доступа в интернет, устройства и используемые протоколы специфичны, да и единственная на то время атака на иранские центрифуги с помощью вируса Stuxnet вызывала сомнения.

Жизнь показала, что скепсис был напрасным. Проблема стала актуальной, а кибербезопасность автоматизированных систем управления технологическими процессами – одним из важнейших направлений обеспечения безопасности страны.

Бизнесу стоит тщательно изучить свою инфраструктуру, провести учет доступных через интернет устройств, ограничить удаленный доступ и, принимая во внимание текущие геополитические риски, посмотреть на решения зарубежных поставщиков. Оценивший преимущества цифровизации бизнес не заставишь отказаться от интернета и цифровых технологий. Но минимизировать угрозы со стороны киберпространства необходимо. ИКС

ЦОДы и кибербезопасность

Николай Носов

Клиентам ЦОДов нужно иметь объективную оценку безопасности используемой ИТ-инфраструктуры провайдера. Получить такую оценку поможет разработка единого стандарта ИБ и тестирование защиты дата-центров в ходе пентестов и киберучений.

Угрозы растут

Ночь с субботы на воскресенье – лучшее время для хакерской атаки. Руководство жарит шашлыки на дачах, на рабочих местах минимум сотрудников. Неудивительно, что именно воскресным утром 26 мая перестал работать сайт службы СДЭК – одной из самых популярных служб доставки в стране. Компания обещала восстановить сервис не позднее среды, но прием заказов начался только в субботу 1 июня. Потери от срыва сроков доставки у клиентов оценить трудно, но учитывая масштаб работы службы, можно предположить, что они значительные. Ответственность за сбой взяла на себя хакерская группа, сообщившая в соцсети, что якобы зашифровала данные компании. Вне зависимости от того, насколько это утверждение соответствовало действительности, оно еще раз привлекло внимание к теме информационной безопасности предприятий.

Число успешных кибератак растет. Согласно исследованию Positive Technologies «Готовы ли российские компании противостоять кибератакам?», представленному на конференции Positive Hacks Days, с 2019 по 2023 гг. число успешных атак увеличилось более чем на 134%, а средний ущерб, нанесенный хакерами крупным компаниям РФ за период с июля 2022 г. по июнь 2023 г., вырос на треть по сравнению с предыдущим аналогичным периодом и составил не менее 20 млн руб. И это без учета репутационных потерь.

Бизнес информационной безопасностью занимается, но в целом ситуация тревожная. По данным, приведенным старшим аналитиком информационной безопасности исследовательской группы Positive Technologies Федором Чунижековым, 93% организаций не защищены от проникновения злоумышленника внутрь сети, 63% подвержены перехвату контроля над инфраструктурой со стороны злоумышленников даже с низкой квалификацией.

С заботой о главном

Модифицируется и масштабируется инфраструктура, появляются новые уязвимые места, совершенствуются технологии атак. Обезопасить всё нереально – нужно выбирать главное, защищаться от возникновения в результате кибератаки недопустимого события, делающего невозможным достижение операционной или стратегической цели организации. Такие события могут быть специфичными, связанными с особенностями конкретной компании, но чаще они типичны, по крайней мере для отрасли. Например, для интернет-магазина недопустимое событие – недоступность сайта вследствие DDoS-атаки.

Для предотвращения недопустимых событий нужна результативная система киберзащиты, на практике обеспечивающая безопасность. Нужны критерии и методы оценки киберустойчивости предприятия – способности поддерживать непрерывность бизнес-процессов в условиях кибератаки. Хорошо, когда такие критерии названы публично и оценки проводятся регулярно, причем независимыми организациями, – это дает представление о надежности киберзащиты выбираемого контрагента.

Наименее затратный метод оценки уровня защищенности, как отмечают в Positive Technologies, – аттестация, которая проводится в основном по представленным документам и подтверждает выполнение организационных и технических требований стандартов или регуляторных норм (рис. 1). «Бумажная безопасность» – разработка документов, приказов, инструкций и технологических регламентов –

важна не только для аттестации и прохождения проверок, но и как основа кибербезопасности. Но все же она только основа, необходимая, но недостаточная для обеспечения киберустойчивости.

Более эффективно применение автоматических сканеров и анализ результатов их работы. Широко используются антивирусные программы с функцией автоматического сканирования системы на предмет вредоносных программ и уязвимостей. Это второй по распространенности (47%) метод оценки защищенности, особенно в компаниях среднего и малого бизнеса.

Самый распространенный метод оценки защищенности – тестирование на проникновение (пентест). Этому методу отдают предпочтение в организациях более половины (58%) респондентов (рис. 2). Проведение пентестов популярно среди компаний всех масштабов.

Треть респондентов (35%) заявила о проведении киберучений – наиболее эффективного метода оценки уровня защищенности. Однако в силу дороговизны и необходимости иметь оснащенный SOC (операционный центр кибербезопасности) с квалифицированным персоналом этот метод отметили только крупные организации.

Самой объективной проверкой киберустойчивости будет способность выдержать реальную атаку хакеров в ходе программы багбаунти. В этом случае организация предлагает вознаграждение за нахождение уязвимостей в ее ПО или веб-приложениях и сообщение о них. Немногие компании (лишь 15%) уверены в своей защите настолько, что заявляют о готовности выдержать атаки хакеров со всего мира. Причем среди этих организаций не только коммерческие (Ozon, Wildberries, Тинькофф), но и государственные структуры (Минцифры России).

Стандарты кибербезопасности для ЦОДов

Ситуация с кибербезопасностью в коммерческих ЦОДах напоминает ситуацию в российских банках 15 лет назад, когда каждый банк по своему усмотрению обеспечивал защиту информационной структуры и фрагментарно аттестовал ее по отдельным стандартам, необходимым прежде всего для работы с западными платежными системами. Оценка уровня кибербезопасности финансовых организаций была непрозрачной не только для клиентов, но и для регуляторов, что сильно беспокоило ЦБ, поскольку новости об успешных атаках на отдельные банки подрывали доверие к финансовой системе в целом.

Чтобы исправить ситуацию, Банк России разработал комплекс документов для единого подхода к построению ИБ – стандарт Банка России по обеспечению информационной безопасности организаций банковской системы РФ (СТО БР ИББС). Хотя стандарт имеет рекомендательный статус, но если банк его принимает, то выполнение стандарта становится для него обязательным, а у ЦБ хватает рычагов, чтобы банки «добровольно» делали правильный выбор. Регулятор не только выпускает стандарты и отчетные формы, но и контролирует их выполнение в ходе проверок. В итоге последний известный полноценный (с уводом денег с корсчета) взлом российского банка произошел девять лет назад, а финансовая отрасль стала одной из наиболее защищенных от киберугроз в стране.

Банки – сердце традиционной экономики, основа финансовой системы, связывающей предприятия разных сфер бизнеса. ЦОДы – сердце новой экономики, экономики данных, они перекачивают связывающие предприятия потоки информации. Поэтому отношение к их кибербезопасности должно быть не менее ответственным, чем к банковской.

Киберзащита ЦОДов должна учитывать специфику этих объектов, обусловленную наличи-

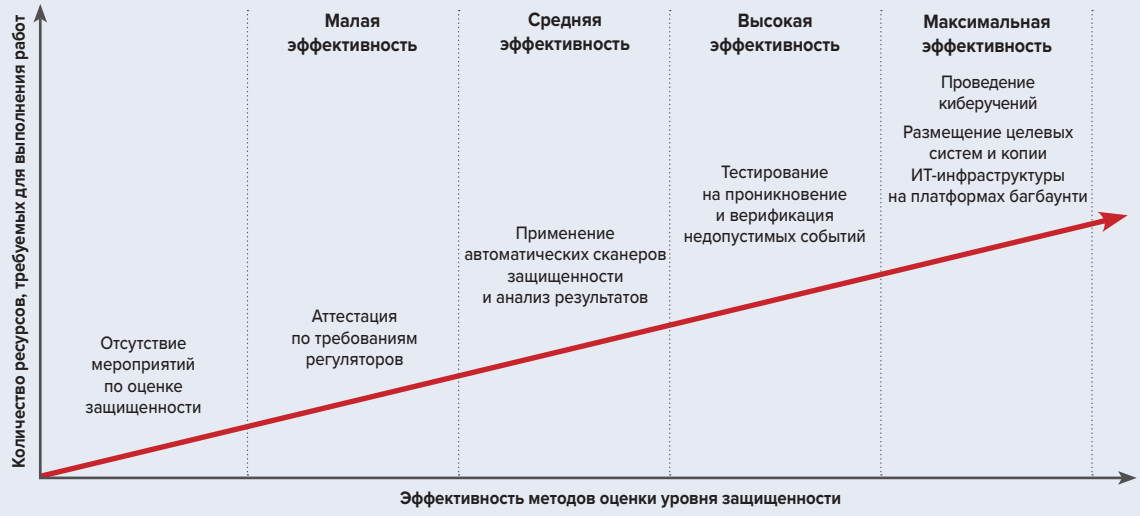
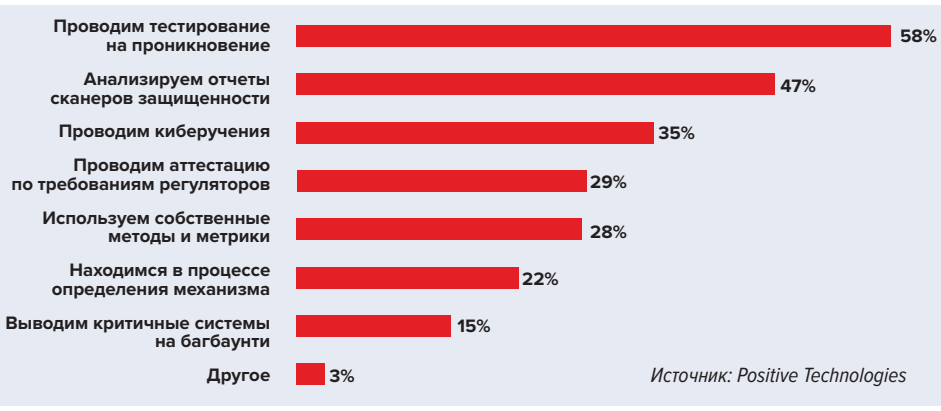


Рис. 1. ▶ Эффективность методов оценки уровня защищенности предприятий

Источник: Positive Technologies



▲ **Рис. 2**
Как организации оценивают уровень защищенности и способность противостоять кибератакам (доля участников опроса)

ем в дата-центре независимых клиентов, имеющих свою ИТ-инфраструктуру, и разными моделями предоставления услуг (colocation, IaaS, PaaS, SaaS), которые предполагают разное разграничение ответственности. Если в рамках модели colocation ЦОД отвечает только за физическую безопасность, то в рамках SaaS – уже за кибербезопасность всей ИТ-инфраструктуры.

Может быть, Минцифры стоит присмотреться к опыту Банка России и разработать свой «СТО БР ИББС», только для ЦОДов? Во всяком случае это обеспечит реализацию мер «бумажной безопасности» – в каждом ЦОДе будет утверждена общая политика безопасности, политики безопасности по отдельным направлениям (физическая, разграничение доступа, защита от DDoS...), разработана модель угроз, приняты документы, определяющие коммерческую тайну, регламенты, технологические инструкции. Для начала необязательно, подобно Банку России, проводить постоянные проверки. Достаточно, например, чтобы дата-центры хотя бы раз в год подтверждали свое соответствие стандарту – это уже стало бы маркером для клиентов и давало конкурентное преимущество на рынке.

Справедливости ради надо сказать, что многое у ЦОДов и так есть, особенно у тех, кто предоставляет услуги безопасности из облака по модели SECaaS. Ведь эти же инструменты, как правило, используются провайдером и для защиты собственной инфраструктуры. А если ЦОД предоставляет клиенту инфраструктуру, соответствующую требованиям закона № 152-ФЗ (защита персональных данных) или № 187-ФЗ (обеспечение безопасности КИИ), то выполняет и нужные регуляторные требования.

Если ЦОД предоставляет услуги ГИС, то он должен заранее соответствовать жестким требованиям регулятора. Согласно Постановлению Правительства РФ от 11.05.2017 № 555, вопросы информационной безопасности следует решить до ввода ГИС в промышленную эксплуатацию.

Если ЦОД обслуживает финансовые организации, то его инфраструктура сертифицирована в соответствии с требованиями международного стандарта безопасности платежных данных PCI DSS (Payment Card Industry Data Security Standard). Сертификат соответствия PCI DSS содержит технические и организационные требования, необходимые для безопасной обработки данных о держателях платежных карт и гарантирует, что клиенты ЦОДа могут обрабатывать их в соответствии с международным стандартом без угрозы утечки и нарушения законодательных норм.

Сертификация по отдельным направлениям важна, но не обеспечивает кибербезопасности объекта в комплексе, именно как дата-центра. Тем более что управление кибербезопасностью, как это делает Банк России в отношении финансовой системы, не сводится к разовому выпуску стандарта – это процесс, который подразумевает постоянную разработку новых документов, отвечающих меняющемуся ландшафту угроз.

Проверка боем

На киберполигоне Standoff, развернутом на Малой спортивной арене Лужников во время Positive Hack Days, было жарко. Команды «красных» атаковали банки, ЖКХ, системы управления поездами и даже АЭС. Команды «синих» изучали тактики «белых» хакеров и совершенствовали системы защиты. Среди них были представители разных отраслей и даже решившие проверить свои системы на киберустойчивость безопасники из экзотических стран. Не было только представителей дата-центров.

Разработать, развернуть и наладить постоянную работу систем защиты необходимо. Но не менее важно их постоянно проверять, в том числе ЦОДам. Заказывать тесты на проникновение, включая физическое (услуга, которую уже рекламировали на рынке), проводить киберучения и программы багбаунти. Причем делать это регулярно. Тогда появится уверенность в киберустойчивости своего ЦОДа – и, что еще важнее, такая уверенность появится у клиентов. ИКС

Линейка серверных шкафов для ЦОДов

Компания «МИКсистем» начала производство обновленной линейки серверных шкафов «Колокейшен», основой для которой стал ее серверный шкаф серии PRO.

Шкаф «Колокейшен» в серийной версии имеет следующие габаритные размеры: высота – 42U или 48U, глубина – 1070 или 1200 мм, ширина – 600, 750 или 800 мм. Он оснащается одностворчатыми или двустворчатыми дверьми с легкосъемными петлями, с процентом перфорации 85% и углом открытия 150 градусов.

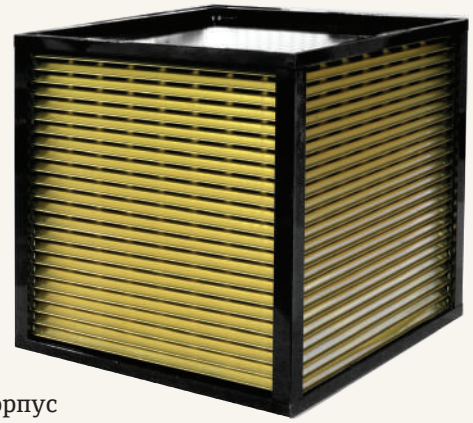
Шкаф имеет два раздельных отсека с индивидуальным доступом, раздельные кожухи для кабельных сборок, усиленные ножки и ролики для оперативного перемещения. Максимальная динамическая нагрузка – 1200 кг, максимальная статическая нагрузка – 2000 кг.

Модель шкафа окрашена порошковой краской черного цвета (RAL 9005) с предварительным фосфатированием поверхности.

Новая версия шкафа «Колокейшен» от «МИКсистем» имеет необходимый сертификат соответствия. На изделие предоставляется расширенная пятилетняя гарантия.

www.metalkomp.ru

Рекуператор для систем непрямого испарительного охлаждения ЦОДов



Российская компания «Панова Тех» с 2024 г. производит на автоматизированной роботизированной линии пластинчатые рекуператоры, являющиеся ключевым элементом систем непрямого испарительного охлаждения (косвенного фрикулинга).

Рекуператоры RPX–ZE представляют собой набор штампованных алюминиевых пластин, собираемых в пакет с двойным замковым соединением. Пластины различаются высотой выштампованных элементов в зависимости от требуемого шага пластин и соединяются между собой методом двойной фальцовки. В результате на входных и выходных гранях пакета пластины имеют замковое соединение толщиной, равной пятикратной толщине пластины, что обеспечивает высокую прочность и герметичность конструкции пакета.

Собранный пакет пластин устанавливается в стандартный корпус с модернизированными стойками. Стойки рекуператора изготавливаются из профилированного алюминия, позволяющего максимально эффективно использовать площадь «живого» сечения, обеспечивая герметичность и исключая скопление конденсата и появление неприятного запаха в системе приточной вентиляции. Алюминиевые пластины и корпус имеют эпоксидное покрытие.

Рекуператоры RPX-ZE обеспечивают эффективность рекуперации до 70% и внутренний переток воздуха не более 0,1%.

Все технические параметры рекуператоров, в том числе эффективность рекуперации и падение давления, проверяются на специализированном стенде по методикам стандартов Eurovent. Стенд оснащен высокоточными средствами измерений, вентиляционным оборудованием и системой автоматики, способными стабильно поддерживать расход, температуру и влажность подаваемого в рекуператор воздуха в широком диапазоне режимов испытаний.

www.panovatech.ru

Энергомодули высокой заводской готовности

Компания ART Engineering представляет энергомодули серии TownScape – системы гарантированного электроснабжения контейнерного типа. Решение актуально для научных, торговых и производственных предприятий, медицинских учреждений, банков и государственных структур, а также для ЦОДов.

Энергомодули являются предсобранными изделиями (префабами) и поставляются заказчику полностью готовыми к эксплуатации.

Внутри энергомодулей TownScape установлены источники бесперебойного питания общей мощностью до 1,5 МВт. Для обеспечения непрерывной работы модули оснащены комплексом инженерных систем, а именно: системами прецизионного кондиционирования воздуха, дежурного и аварийного освещения, пожарно-охранной сигнализации и пожаротушения, дистанционного мониторинга, внутреннего распределения электроэнергии, а также системой отопления и вентиляции.

Энергомодули изготавливаются и проходят все необходимые испытания на собственной площадке ART Engineering в Рязани. Доставка к месту эксплуатации возможна любым видом транспорта. Пусконаладочные работы на объекте занимают 7 дней. Срок поставки энергомодуля – от 3 месяцев, а гарантия – до 3 лет.

art-engineer.ru

Высокопроизводительные свинцово-кислотные АКБ

ГК «Вектор Энерджи» предлагает высокопроизводительные свинцово-кислотные аккумуляторные батареи VEKTOR ENERGY серии High Rate (HRL), изготовленные по технологии AGM и предназначенные для работы в составе ИБП.

АКБ серии High Rate разработаны специально для применения в энергоемких системах бесперебойного питания ЦОДов и различного высокотехнологичного оборудования. Достоинство этих аккумуляторов заключается в способности отдавать большой ток за короткий промежуток времени (5–15 мин). Кроме того, они отличаются высокой удельной плотностью энергии и низким внутренним сопротивлением, а также обладают низким саморазрядом.

Аккумуляторы серии High Rate имеют увеличенное количество пластин – для увеличения общей площади поверхности и улучшения способности к разряду большим током (технология HPD), а также более толстые шины. Для повышения устойчивости к кислотной коррозии пластинчатая решетка изготавливается из специального сплава (технология SPA). При нанесении пасты активного вещества на свинцовые пластины применяются двойная прокатка и сушка, благодаря чему активное вещество наносится плотнее. Это, в свою очередь, обеспечивает более плотную сборку положительных и отрицательных пластин/электродов, за счет чего уменьшается внутреннее сопротивление аккумулятора. Все это обеспечивает отдачу большей мощности, а также способствует увеличению срока службы АКБ до 15 лет.

www.vektor-energy.ru

РЕКЛАМА В НОМЕРЕ

НЕД-ЦЕНТР
Тел.: (800) 555-8448
E-mail: ned@air-ned.com
www.air-ned.com ..... с. 44–45

СВОБОДНЫЕ ТЕХНОЛОГИИ ИНЖИНИРИНГ
Тел.: (495) 120-2866
E-mail: info@sv-tech.ru
www.sv-tech.ru ..... с. 49

СДИ СОФТ
Тел.: (499) 495-1042
E-mail: info@sdisoft.ru
https://sdisoft.ru/ ..... с. 50–51

ALCON GROUP
Тел.: (495) 967-6923
E-mail: info@alcongroup.ru
https://alcongroup.ru/ ..... с. 26–27

ХАЙТЕД
Тел.: (495) 789-3800
E-mail: info@hited.ru
www.hited.ru ..... с. 56–57

CLIVET РОССИЯ
Телефон: (495) 646-2009
E-mail: info.ru@clivet.com
www.clivet.com ..... 2-я обл., с. 34–35

EKF
Тел.: (800) 333-8815
E-mail: info@ekf.su
https://ekfgroup.com/ ..... с. 55

KEY POINT
Тел.: (495) 120-2866
E-mail: info@keypoint-group.ru
https://keypoint-group.ru/ .... с. 8–9, 4-я обл.

POWERCOM
Тел: (495) 651-6281
Факс: (495) 651-6282
Email: sales@pcm.ru
www.pcm.ru ..... с. 36–37

TERMOINDUSTRY
Тел.: (800) 100-3845
E-mail: info@termo-industry.ru
https://termo-industry.ru/ ..... с. 64–65

SYSTEME ELECTRIC
Тел.: (495) 777-9990
E-mail: ru.ccc@se.com
www.systeme.ru ..... 1-я обл., с. 20–21

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.

7–10 октября 2024

Неделя ЦОДов
и облачных технологий

Data Center & Cloud Kazakhstan

Казахстан, Алматы
The Rixos Hotel Almaty

4–5 ноября 2024

Евразийский форум по ЦОДам
и облачным технологиям

Eurasia Data Center & Cloud Forum

Узбекистан, Ташкент
Hilton Tashkent City

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

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

ПОДРОБНО О ПРОГРАММЕ И УЧАСТНИКАХ
НА САЙТАХ КОНФЕРЕНЦИЙ

DCFORUM.KZ

DCFORUM.UZ

**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

Ассоциация операторов ЦОДов и облачных сервисов Казахстан

uptime INSTITUTE

KEY POINT GROUP

РЕГИОНАЛЬНАЯ СЕТЬ ЦОД ГРУППЫ КОМПАНИЙ KEY POINT

ВАЖЕН КАЖДЫЙ!

ДАТА-ЦЕНТРЫ С СЕРТИФИКАЦИЕЙ TIER III

keypoint-group.ru