

ТЕМА НОМЕРА

ЦОД – ОТЕЧЕСТВЕННЫЙ НА 70%. КОГДА?

Цифровые сервисы в туризме	28	Надежность гибридных сред	79
Гиперконвергенция и СХД	70	Аутентификация на раз-два	84
Цифровизация медицины	72	Чек-лист безопасности облаков	92

ИнформКурьер-Связь

ИКС

издается с 1992 года

Евгений Богданчиков

*Исполнительный
директор DataPro*

**Наша цель – построить
лучшую компанию на рынке
дата-центров России**



2-й ОНЛАЙН-ФОРУМ

9 декабря 2021

Онлайн-форум посвящен вопросам надежности и отказоустойчивости ЦОДов – важнейшим факторам выживания и развития бизнеса в современном мире. Перебои в получении ИТ-сервисов чреваты потерей ценной информации, финансовыми убытками и даже техногенными катастрофами.

На форуме речь пойдет об основных элементах ИТ- и инженерной инфраструктуры, их проектировании и создании, способах повышения живучести.



Актуальность

Надежность функционирования ИТ как основа производственных и бизнес-процессов, государственного управления



Студийный формат

Эксперты соберутся в студии в Москве, а их выступления и дискуссии будут транслироваться в интернет



Целевая аудитория

ИТ-директора, руководители и специалисты компаний крупного и среднего бизнеса

ОРГАНИЗАТОР



ПРИ ПОДДЕРЖКЕ



Минцифры
России



КООРДИНАЦИОННЫЙ СОВЕТ
ПО ЦОДАМ И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ
Автономная некоммерческая организация

Реклама

ЗАРЕГИСТРИРОВАВШИМСЯ БУДЕТ ДОСТУПНА
ВИДЕОЗАПИСЬ НА САЙТЕ КОНФЕРЕНЦИИ



event.iksmedia.ru

16+

Издается с мая 1992 г.

Издатель
ООО «ИКС-Медиа»участник
АНО КС ЦОДКООРДИНАЦИОННЫЙ СОВЕТ
ПО ЦОДАМ И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ
Автономная некоммерческая организация

Генеральный директор

Д.Р. Бедердинов
dmitry@iks-media.ru

Учредители:

ООО «ИКС-Медиа»,
МНТОРЭС им. А.С. Попова

Главный редактор

А.Г. Барсков
a.barskov@iks-media.ru

РЕДАКЦИЯ

iks@iks-media.ru

Ответственный редактор

Н.Н. Шталтовная
ns@iks-media.ru

Обозреватель

Н.В. Носов
nikolay.nosov@iks-media.ru

Корректор

Е.А. Краснушкина

Дизайн и верстка

Е.В. Денисова

КОММЕРЧЕСКАЯ СЛУЖБА

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

СЛУЖБА РАСПРОСТРАНЕНИЯ

Выставки, конференции
expo@iks-media.ru
Подписка
podpiska@iks-media.ru

Журнал «ИнформКурьер-Связь» зарегистрирован в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций 02 февраля 2016 г.; ПИ №ФС77-64804.

Мнения авторов не всегда отражают точку зрения редакции. Статьи с пометкой «бизнес-партнер» публикуются на правах рекламы. За содержание рекламных публикаций и объявлений редакция ответственности не несет. Любое использование материалов журнала допускается только с письменного разрешения редакции и со ссылкой на журнал.

Рукописи не рецензируются и не возвращаются.

© «ИнформКурьер-Связь», 2021

Адрес редакции и издателя:

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

№4/2021 подписан в печать 29.10.21.

Тираж 8 000 экз. Свободная цена.

Формат 64x84/8

ISSN 0869-7973

12+

Принципы ESG и показатель PUE



На повестку дня, в том числе в России, подняты принципы ESG (Environmental, Social, Governance), которые у нас почему-то называют устойчивым развитием. Наверное, правильнее говорить о гармоничном или социально ответственном развитии. Но, как ни называй, тема эта неразрывно связана с экологией, а значит, с потреблением энергии ЦОДами.

А потребление быстро растет. Если усреднить многочисленные оценки, то сегодня ЦОДы по всему миру «съедают» 1–2% генерируемой энергии, но уже к 2030 г. цифра вырастет на порядок. Из этого есть несколько важных следствий. Первое – дата-центры превратятся в крупнейших потребителей электричества. Значит, из обычных покупателей они неизбежно станут партнерами энергосетей и в рамках партнерства начнут помогать стабилизировать работу энергосетей и поставлять энергию в пиковые периоды (**ЦОД от концепции до модернизации**).

Второе следствие – рост внимания к ЦОДам со стороны экологов. Уже есть примеры нормативного ограничения развития отрасли дата-центров. Так, в Амстердаме в 2020 г. не разрешали строительство новых ЦОДов, за исключением случаев, когда строящая объект компания гарантировала, что показатель его энергоэффективности (PUE) не превысит 1,2. Значит, если ЦОДы не хотят, чтобы «зеленые» блокировали объекты с плакатами «Закрой ЦОД – спаси планету», они должны становиться более энергоэффективными.

Но с этим пока проблемы. Средний PUE уже почти восемь лет особенно не падает. По данным Uptime Institute, до 2014 г. наблюдалось его быстрое снижение (до 1,65), к 2018 г. он еще немного уменьшился (до 1,58) и вышел на плато – в 2021 г. средний PUE составил 1,57. Согласитесь, это намного выше уровня 1,2, который был обязателен для новых дата-центров в Амстердаме.

Причин стабилизации PUE несколько. Во-первых, отрасль ЦОДов выработала некоторые типовые технологические решения, которые устраивают всех, прежде всего с экономической точки зрения. Эти решения обеспечивают тот самый средний PUE на уровне 1,5–1,6. Во-вторых, повышение эффективности почти всегда связано со снижением надежности, а надежность – главный показатель для ответственных ЦОДов.

Кардинальное снижение PUE требует внедрения прорывных решений, в первую очередь в системах охлаждения. Это, например, переход на бескомпрессорные системы с максимальным применением фрикулинга. Но строящиеся сейчас в России крупные объекты в основном задействуют традиционные (компрессорные) схемы. Очередной цикл развития (обновления) ЦОДов начнется года через два-три, а значит, на существенное снижение PUE за счет фрикулинга в ближайшие годы рассчитывать не приходится. Но фрикулинг – далеко не единственный инструмент реализации принципов ESG.

За гармоничное развитие ЦОДов,
Александр Барсков

ЦОД – отечественный на 70%. Когда?

с. 12

1 КОЛОНКА РЕДАКТОРА

4 ИКС-Панорама

- 4 Дата-центры на Шелковом пути
- 6 Российский GitHub, государство и open source
- 8 Рынок дата-центров – рынок продавца
- 11 ДАЙДЖЕСТ ОТРАСЛИ ЦОДов

12 Экономика и бизнес

- 12 А. Барсков. ЦОД – отечественный на 70%. Когда?
- 16 Д. Грачев. Системы хранения данных: сделано в России
- 19 Г. Кашин. Импортозамещение: не забудьте об обучении персонала
- 22 А. Барсков. ГИСы уйдут в коммерческие ЦОДы
- 24 Е. Богданчиков. «Большая тройка» и «большая стройка»
- 26 В. Соловьев. Новая эра: ЭДО в медицинских организациях
- 28 Т. Толмачева, С. Патрикеева. Цифровые сервисы в индустрии гостеприимства: произойдет ли перезагрузка?
- 32 И. Бакланов. Апология инженерии



с. 8 Рынок дата-центров – рынок продавца



с. 32

И. Бакланов. Апология инженерии



А. Барсков. ЦОД от концепции до модернизации



А. Новак. Искусственный интеллект в видеоаналитике. Реальные возможности



О. Ермакова. Закон № 152-ФЗ: что нового в 2021 году?

34 Инфраструктура

- 34 А. Барсков. ЦОД от концепции до модернизации
- 44 А. Ежов. Рядное фреоновое охлаждение: до 69 кВт холода с квадратного метра
- 46 Р. Асьерто, П. Джонсон. Бесперебойное электропитание ЦОДов: тенденции до 2025 года
- 52 Н. Носов. Натрий-ион для дата-центров
- 54 А. Воробьев. Вендор в жизни ЦОДа: помощь на всех этапах
- 56 А. Эрлих, А. Галкина. Гениальность или абсурд? О способах снижения энергопотребления
- 60 В. Воробьев. ЦОД для банка: надежность и масштабируемость
- 62 И. Савинкин. Автоматизация ЦОДа: шесть аспектов проектирования и эксплуатации
- 64 А. Семенов. Как и для чего автоматизировать проектирование СКС
- 68 А. Зуев. EMILINK: производство в России – главное преимущество
- 70 В. Володкович. Гиперконвергенция и СХД: горизонты применения

72 Сервисы и приложения

- 72 А. Дюков. Системы цифровизации здравоохранения: интеграционная платформа vs моноМИС
- 76 А. Залманова. Эффективный переход на отечественную виртуализацию, или Едим слона по частям
- 79 А. Бытин. Распределенные вычисления и надежность гибридных сред
- 82 А. Новак. Искусственный интеллект в видеоаналитике. Реальные возможности

84 Безопасность

- 84 Н. Носов. Аутентификация на раз-два
- 89 О. Ермакова. Закон № 152-ФЗ: что нового в 2021 году?
- 92 А. Ветколь. Чек-лист безопасности облачных сервисов

94 Новые продукты

Дата-центры на Шелковом пути

Рынок ЦОДов среднеазиатских республик значительно меньше российского, но развивается более быстрыми темпами. Использование западного и российского опыта позволит сократить отставание.



Так можно кратко сформулировать основные тезисы организованной «ИКС-Медиа» конференции «ЦОД. Шелковый путь», прошедшей в ставшем уже привычным во время пандемии формате онлайн. За выступлениями экспертов в студиях в Москве и Алматы следили более 500 участников из России и среднеазиатских республик.

Проблемы и достижения Узбекистана

В Узбекистане рынок коммерческих ЦОДов находится на самых ранних стадиях формирования. В 2020 г. там насчитывалось всего 110 стойко-мест, уровень утилизации – 75%. Ожидается, что к 2025 г. число стоек увеличится практически в десять раз. Такой рост во многом объясняется низкой стартовой базой.

Среди особенностей рынка республики ведущий консультант iKS-Consulting Денис Патрикеев отметил слабую развитость отрасли ИКТ, низкий уровень спроса и



дефицит высококачественного предложения. Сильна региональная диспропорция рынка – более 50% ИТ-компаний и пользователей интернета сосредоточено в Ташкенте. Главным драйвером развития и потребителем ИКТ-услуг в целом и цифровой инфраструктуры в частности выступает государство, все три узбекских оператора сотовой связи созданы с его участием.

Уровень конкуренции на ИКТ-рынке низкий: 42% коммерческих стоек принадлежат «Узбектелекому», 23% – Университету Инха в Ташкенте, 12% – «Узинформу». Другие негативные факторы – нехватка специалистов, волатильность национальной валюты и дефицит электрических мощностей.

Однако за последние пять лет в республике произошли значительные изменения, улучшился инвестиционный климат. Страна переживает период экономического роста. Инвестиции в ИТ-сектор за четыре года выросли в четыре раза. В 3,8 раза – с 17,9 до 68,6 тыс. км – выросла протяженность проложенных ВОЛС, причем до конца 2021 г. ее планируется практически удвоить.

Положительное влияние на рынок коммерческих ЦОДов окажут национальная программа «Цифровой Узбекистан 2030», программа «Цифровой Ташкент» и вступившие в силу законодательные требования о хранении персональных данных на территории республики.

Взгляд на Казахстан

Рынок коммерческих дата-центров Казахстана в 10 раз больше, чем у южных соседей, но, как и у них, находится в стадии формирования.

Причем фаза формирования затянулась. Рынку уже 10 лет, но темпы роста остаются умеренными – 16–20%. Доля доходов коммерческих дата-центров в общем «пироге» ИКТ-услуг Казахстана не превышает 3,5%. В целом на рынке ЦОДов первую скрипку играют операторы связи – им принадлежит 80% коммерческих стоек. «Рынок нуждается во внешних драйверах», – считает глава представительства iKS-Consulting в Казахстане Светлана Черненко.

2021 г. обещает стать переломным. Устоявшийся конкурентный ландшафт изменился за счет нескольких знаковых событий. В начале года «Транстелеком» запустил в семи регионах республики семь дата-центров с 96 стойками в каждом с возможностью наращивания до 300. В результате объем рынка увеличился почти на треть. С вводом новых площадок «Транстелеком» стал третьим оператором республиканской сети ЦОДов Казахстана, после «Казахтелекома» и компании «Национальные информационные технологии», а по общему количеству стоек вырвался в лидеры.

Другое заметное событие – появление нового игрока QazCloud, компании, ассоциированной с «Казахтелекомом». Ее новый модульный ЦОД на 100 стоек ориентирован не только на госсектор, но и на бизнес-клиентов. В начале 2021 г. компания «Казтелепорт» анонсировала запуск в



2022 г. дата-центра «Сайрам» в Алматы, который добавится к ее ЦОДам в Алматы и Нур-Султане. В пандемию выросла востребованность вычислительных мощностей. Так, по дан-

Кадр из видеотрансляции



Кадр из видеотрансляции



ным коммерческого директора «Казтелепорта» Игоря Пака, за последний год в компании спрос на аренду CPU увеличился на 178%, RAM – на 107%, HDD – на 157%.

Цифровой Шелковый путь

В древности Европу и Азию связывали караванные пути, в том числе и Великий шелковый путь, проходящий через территории стран бывшего СССР. В компьютерную эпоху пути должны стать цифровыми. Одно из важных направлений цифровой повестки ЕАЭС – формирование цифрового пространства союза, развитие цифровых инфраструктур и экосистем. «Наличие надежных дата-центров в каждой стране ЕАЭС – фундамент для развития экономики данных», – отметила управляющий партнер iKS-Consulting Татьяна Толмачева.

Сравнительный анализ рынков Казахстана, Узбекистана и России показывает неравномерность развития цифровых инфраструктур, отставание Казахстана от России и Узбекистана от Казахстана. Если в России спрос на услуги ЦОДов оценивается в 9 000 новых стоек в год, то в Казахстане – в 200–300, а в Узбекистане – около 100 стоек в год. В России активнее используют облачные сервисы, выше требования к их качеству.

Цифровая прозрачность инфраструктуры

Однако лаг в развитии среднеазиатских республик имеет свои плюсы: можно воспользоваться опытом, накопленным западными и российскими компаниями, ориентироваться на принесшие успех бизнес-модели, применять самые современные технологии. Именно на это нацелено сотрудничество с ведущими вендорами.

«Заказчики все больше делают упор не на отдельные характеристики оборудования, а на показатели ЦОДа в целом: надежность и энергоэффективность, которая складывается из энергоэффективности систем энергоснабжения и охлаждения, а также правильного использования серверного оборудования. Показатели рассматриваются в комплексе», – указал технический директор подразделения Secure Power компании Schneider Electric Алексей Соловьев. Нужна единая стратегия развития вычислительной среды, «цифровая прозрачность» всей инфраструктуры и проактивный сервис – проще предотвратить аварию, чем ликвидировать ее последствия. Для решения этих задач компания предлагает EcoStruxure – облачное решение по управлению инфраструктурой центров обработки данных и комплексные решения InfraStruxure.

Прозрачность нужна и для сети. Она, в частности, поможет понять, почему пользователь жалуется на недоступность сервиса или слишком большие задержки, когда сигналов об ошибке нет. «Чтобы решить проблему, стали развивать направление сетей, ориентированных на пользовательский опыт», – пояснил менеджер по маркетингу компании Juniper Павел Борох. Под пользовательским опытом понимается опыт двух категорий – служб эксплуатации сетей и конечных пользователей. Решения Juniper помогают создать сеть для ЦОДа с заданной производительностью, выявлять аномалии и делать прогнозы на основе систем аналитики с использованием искусственного интеллекта, автоматически исправлять ошибки, динамически обеспечивать защиту и соблюдение политик безопасности.

Цифровая зависимость или взаимовыгодное сотрудничество?

После того, как премьер-министр Казахстана и глава Сбера в ходе Восточного экономического форума подписали меморандум о сотрудничестве, обострились существовавшие и до этого опасения «цифровой колонизации» среднеазиатских республик. Документ описывает ключевые подходы к развитию сотрудничества с целью внедрения в Казахстане цифровой платформы GovTech, реинжиниринга и цифровой трансформации госуправления с применением практик анализа данных и искусственного интеллекта. Критики, в частности, утверждают, что при реализации проекта Казахстан попадет в цифровую зависимость от России с точки зрения цифрового менеджмента, кибербезопасности и госадминистрирования. Оппоненты возражают, что никакие персональные данные в Россию передаваться не будут, развивать и дорабатывать созданную Сбером платформу и предоставлять сервис будут местные компании.

Участники дискуссии, прошедшей на конференции «ЦОД. Шелковый путь» в форме телемоста между студиями в Москве и Алматы, не разделили опасений по поводу зарубежных компаний. «Прихода зарубежных игроков не избежать, и мы к этому готовы. В первую очередь мы видим не угрозы, а перспективы, возможности быстрее нарастить компетенции», – заявил И. Пак.

Ни одна страна в мире не имеет полного цифрового суверенитета, все мы связаны друг с другом и используем наработки соседей по планете для быстрого развития своих систем.

Николай Носов



Российский GitHub, государство и open source

В центре дискуссий прошедшего в Москве Russia Open Source Summit была стратегия развития программного обеспечения с открытым кодом в России до 2024 г. Споры шли вокруг структуры проекта, используемой терминологии и роли государства.

Государство и бизнес

По мнению заместителя министра цифрового развития, связи и массовых коммуникаций РФ Максима Паршина, одна из основных целей стратегии – распределение ролей между сообществом разработчиков открытого ПО и государством, которое должно не мешать, а помогать, вовлекать, создавать возможности и регулировать. Помогать в том числе заказами, ведь государство – крупный потребитель продукции open source.



М. Паршин

В рамках госзаказов пишутся миллионы строк кода. Но разработчики часто изобретают велосипед, создают то, что уже было создано ранее. «Большая часть соответствующего кода должна распространяться по открытой лицензии, быть доступна в публичных репозиториях и обязательна для использования другими органами власти при разработке и совершенствовании необходимых им продуктов», – заявил М. Паршин.

Свои взгляды на роль государства в регулировании свободного программного обеспечения (СПО) высказали и разработчики. «Мы были бы рады, если бы государство помогло повысить ценность open source в глазах бизнеса, отрегулировало его использование в государственных информационных системах и сформулировало требования к нему. Например, установило бы, что СПО должно обладать определенным набором качеств. В частности, должны существовать компании, разрабатывающие его в России, устраняющие замечания и неисправности и выпускающие его обновления. И за всем этим кто-то должен следить», – считает генеральный директор компании BellSoft Александр Белокрылов.

В рамках регулирования СПО придется искать баланс между интересами эксплуатантов и разработчиков. Однако эксплуатанты могут быть одновременно и разработчиками. Например, департаменты информационных технологий субъектов РФ в основном эксплуатируют СПО, но часть библиотек могут разрабатывать сами и отдавать в сообщество. «Тут может возникнуть коллизия: все ФОИВ и РОИВ выполняют строго определенные функции и никому не вменено в обязанность разрабаты-

вать ПО для внешних пользователей», – дал комментарий нашему изданию руководитель направления Российского национального коммерческого банка Михаил Орешин.

«Этот саммит ценен тем, что государство впервые обратилось к разработчикам open source, – отметил генеральный директор Postgres Professional Олег Бартунов. – Надеюсь, участники сумели дать понять, что open source надо не руководить, а создавать условия для развития». Авторитетнейший эксперт рынка критически высказался о проекте стратегии: «Документ надо сильно сократить. Стратегия должна быть как скелет, как общий недетализированный план достижения цели – развития программного обеспечения с открытым кодом в России. В ней не должно быть конкретных мер. Кроме того, сейчас проект больше о бизнесе. А open source – это прежде всего люди».

Нужна нормативная база

СПО не синоним бесплатного ПО и ПО без наложенных ограничений. «Свободное» означает только, что распространяются все исходные коды. Но надо разделять код и нематериальные активы. Есть открытый софт, который всегда будет бесплатным и будет распространяться из

открытых источников. А есть софт по открытой лицензии, в рамках которой правообладатель может накладывать те или иные ограничения.

«В принципе различия понятны, но у нас отсутствует нормативная база. Определения нужно зафиксировать в федеральных законах или приказах Минцифры. Чтобы все жили в едином поле, – уверен М. Орешин. – Сейчас под open source чаще



М. Орешин

всего понимают модель распространения кода по открытой лицензии. Но эта лицензия кому-то принадлежит. Не было прецедентов, чтобы старые лицензии отзывали, но новые версии могут лицензироваться по-другому».

Например, Red Hat после покупки ее IBM перестала бесплатно выкладывать сборку операционной системы Linux. Если кто-нибудь хочет собрать сам – все коды доступны. Но вести сборку для промышленной эксплуата-

**О. Бартунов**

ции на постоянной основе – задача не простая.

Одна из предложенных в проекте мер – «разработка отечественных открытых лицензий, учитывающих интересы Российской Федерации в части языка, юрисдикции и правоприменения, и рекомендаций по их применению». «Важна юридическая составляющая – лицензионная чистота и лицензионное приземление внутри нашей страны использования open source», – заявил директор АНО «Центр компетенций по импортозамещению в сфере ИКТ» Илья Массух.

О. Бартунов не поддерживает идею создания русского аналога GPL. «Мир open source-лицензий и так сложный, разобраться в них нелегко. Можно перевести имеющиеся на русский язык, но создавать новые не стоит», – считает он.

Православный GitHub

В кулуарах обсуждалось предложение о создании доверенного национального облачного сервиса публичных репозиторий. По такому пути уже пошел Китай, создавший репозиторий Gitee, местный аналог американского GitHub.

Доступ к продуктам open source может оказаться подвержен санкционным ограничениям. «Если выйдешь в GitHub из Крыма, то аккаунт могут заблокировать. Сам с таким сталкивался. Так что важно иметь российский аналог GitHub. Причем нужна именно среда разработки, а не хранилища, которые у нас уже есть. Выкладывать туда код, который создается по госпрограммам и который сейчас не так легко получить», – пояснил М. Орешин.

«Идея “православного” GitHub, возможно, имеет право на существование, но переносить в него, например, репозиторий Open Java Development Kit нецелесообразно. Мы всё разрабатываем в GitHub, вместе с мировым сообществом, с Oracle, Red Hat, Google и IBM. Это прямые конкуренты, но базовая технология Java нужна всем. Пока нет ограничений, отказываться от совместной разработки не имеет смысла. Возможность использования результатов работы сообщества – огромное преимущество открытых технологий», – указал А. Белокрылов.

**А. Белокрылов**

При этом в BellSoft есть актуальное «зеркало» Open JDK, и в случае введения санкций и ограничений код у компании останется. У нее достаточно ресурсов, чтобы при отключении от

мирового сообщества поддерживать локальное «зеркало». По мнению руководителя BellSoft, отечественный GitHub может иметь смысл для чисто российских проектов, в частности для переиспользования кода, разработанного за бюджетные средства. Из государственных информационных систем надо выделять кроссиндустриальные части и поддерживать их силами нескольких компаний.

О. Бартунов высказал сомнение в привлекательности русского GitHub для наших разработчиков, подчеркнув, что это прежде всего социальная сеть, место, где можно обмениваться идеями, в том числе с зарубежными партнерами. Но если российский аналог GitHub будет предоставлять разработчикам вычислительные мощности, то интерес к нему вырастет. Ведь компании не могут владеть всеми видами «железа» на всех платформах и в нужном количестве. Если сервис обеспечит тестирование, проверку и оценку производительности, будет выявлять уязвимости в коде, это привлечет людей.

Курс на open source

Модель open source доказала свою жизнеспособность и охватила практически все направления в ИТ. Лидеры проприетарного ПО регулярно сообщают о поддержке все новых open source-сообществ, в которые вкладывают огромные деньги. В сообществах работают лучшие профессионалы компаний, получая при этом по основному месту

**Э. Лысенко**

службы вполне «проприетарные» зарплаты. Активно, особенно после начала «войны санкций», осваивают open source российские компании и государственные организации.

Руководитель Департамента информационных технологий Москвы Эдуард Лысенко подчеркнул, что ДИТ уже много лет проводит политику замещения проприетарного ПО открытым. И выступает не только

как потребитель, но и как разработчик, причем делится кодом своих систем с регионами.

Заместитель директора департамента ИТ банка ВТБ Михаил Хазин отметил, что банк не только использует OpenStack, но и отдает свои разработки в сообщество. А «Яндекс», по словам руководителя проекта «Яндекс.Облако» Алексея Башкеева, входит в топ-150 компаний мира по количеству контрибьюторов в разные проекты open source.

Модель open source стала технологическим драйвером в разработке ПО. Сообщество разработчиков открытого ПО уже не ассоциируется с кучкой идеалистов, дарящих миру свои программы. Это бизнес, который имеет свои модели монетизации и в котором заинтересованы и общество, и государство.

Николай Носов



Рынок дата-центров – рынок продавца

Российский рынок ЦОДов достиг зрелости, уверенно растет и в условиях повышенного спроса стал рынком продавца – таков главный вывод 16-й международной конференции и выставки «ЦОД», организованной в Москве «ИКС-Медиа».

Мероприятие собрало свыше 1700 делегатов, более половины участвовали очно.

«Рынок ЦОДов вошел в стадию зрелости», – констатировал ведущий консультант аналитического агентства iKS-Consulting Станислав Мирин. Выросло число слияний и поглощений, выделилась пятерка лидеров, занимающая 57% рынка. На первом месте по числу стоек с большим отрывом идет «Ростелеком-ЦОД», продолжающий наращивать свой потенциал. За DataPro и IXcellerate тянутся Selectel и МТС (с приобретенными ею дата-центрами «Авантаж» и GreenBushDC).

Несмотря на отдельные успешные региональные проекты, доминирование Москвы усиливается. На долю столицы приходится почти три четверти рынка дата-центров. Причем дефицит предложения таков, что стойко-места в новых ЦОДах раскупаются еще на стадии их строительства. Сегодня на фоне явной нехватки вычислительных мощностей бесспорно сложился рынок продавца, который может диктовать условия покупателям. Дефицит наблюдается и на рынке комплектующих. Кроме того, очевидно, что даже после окончания пандемии многие сотрудники останутся на удаленной работе и потребность в облачных сервисах сохранится, поэтому спрос еще долго будет превышать предложение.



Сюй Хай

Мировые тенденции

Глобальный рынок дата-центров также продолжает расти. Причем по прогнозу, который представил генеральный директор подразделения Digital Power компании Huawei в Евразии Сюй Хай, число стоек в мире в 2025 г. достигнет 24 млн. Драйверами быстро развивающегося рынка ЦОДов выступают облачные вычисления, искусственный интеллект и 5G. Среди трендов мировой индустрии ЦОДов китайский эксперт выделил повышение энергоэффективности (снижение PUE), сокращение углеродных выбросов и использование высоконагруженных стоек (правда, в России этот тренд пока не очень силен). Кроме того, Сюй Хай отметил повышение гибкости/масштабируемости, безопасности и надежности дата-центров, скорости их возведения, цифровизацию всех этапов строительства и эксплуатации ЦОДов и внедрение более простых архитектур. В технологическом плане заметны переход от свинцово-кислотных к литий-ионным батареям, более широкое применение фрикулинга и систем на основе искусственного интеллекта.

Новый генеральный директор компании IXcellerate Андрей Аксенов в своем первом публичном выступлении перед столь представительной аудиторией подчеркнул возросший спрос на «зеленые» ЦОДы, ответственно относящиеся к расходованию электроэнергии. Кроме того, он указал на развитие дата-центров за пределами рынков FLAP (Франкфурт, Лондон, Амстердам, Париж), общая мощность которых выросла за последний год на 490 МВт и достигла 2000 МВт. В числе новых направлений – Восточная Европа и Россия. Занимающая пятое место в Европе по концентрации коммерческих дата-центров Москва оказывается в этом контексте перспективной периферией.

Еще одна тенденция – переход к резервированию на уровне ЦОДов. В ее русле работает и сама IXcellerate, купившая землю на юге Москвы, где строит кампус Moscow South – крупнейший коммерческий кампус ЦОДов с перспективой расширения до 20 тыс. стойко-мест. После ввода в строй южной локации клиентам будет доступно резервирование на уровне дата-центров.

Законодателем моды может стать и российская компания DataPro, которая сделала ставку на строительство ЦОДов максимального уровня надежности Tier IV. ЦОД DataPro II на 1600 стойко-мест в Химках стал, по утверждению исполнительного директора компании Евгения Богданчикова, первым российским ЦОДом уровня Tier IV. Но на этом компания не остановится. Ее CEO анонсировал строительство первой в Европе сети коммерческих дата-центров Tier IV. После завершения строительства в 2025 г. ЦОДа DataPro VI общее количество стойко-мест в кластере высоконадежных дата-центров компании достигнет 20 тыс.

«Пандемия подчеркнула необходимость удаленной работы», – отметил главный инженер Citrix Сергей Халяпин. Согласно приведенным им оценкам, 48% сотрудников продолжают работать удаленно по крайней мере часть времени, даже при открытии офисов. А 87% компаний в ближайшей перспективе ускорят миграцию своих инфраструктур в облака. Любой пользователь должен иметь возможность выполнять любую работу с любого устройства в любое время. И использовать при этом любые сервисы и архитектуры – облачные, гибридные, on-premise, монолитные и микросервисные. В этом помогут решения для организации удаленного

доступа Citrix, которые можно строить в стиле Lego, исходя из требований заказчика.

Цифровизация сегодня

«Год назад много говорили о начале цифровизации. Сейчас она действительно наступила. Добегает волна, которая задержалась в 2020 г.», – заявил Кирилл Дмитриев, главный технический специалист по ИТ-проектам компании Rittal. Переходящим «на цифру» производствам для внедрения роботизированных устройств и других инновационных технологий нужны edge-ЦОДы, которые должны быть способны работать в неблагоприятных условиях. Для таких применений Rittal разработала решения с высокой степенью защиты (IP55). В частности, компания представила компактное промышленное решение 24U IP55. Развитие edge-ЦОДов – тренд не новый, но по-прежнему актуальный.

Цифровая трансформация меняет ИТ-инфраструктуру ЦОДов, требует новых подходов в управлении. Вице-президент по сервису Schneider Electric Александр Саванович рассказал о разработках компании для обслуживания инфраструктуры, которые помогают в паспортизации объектов, уменьшая влияние человеческого фактора. Программная платформа ETAP позволяет создавать цифровой двойник объекта, принимать решения на его основе при проектировании и эксплуатации. Системы удаленного мониторинга и предиктивной аналитики EcoStruxure Asset Advisor и EcoStruxure IT Expert обеспечивают обслуживание оборудования не по графику, а по состоянию. Упрощает обслуживание система дополненной реальности EcoStruxure Augmented Operated Advisor.

Последний оплот защиты

Пожар в ЦОДе в Страсбурге привлек внимание к системам резервного копирования. Мало интересоваться числом девяток в показателях надежности дата-центра. В случае аварии это не вернет данные, а провайдер отдается суммой, зафиксированной в SLA и несопоставимой с ущербом от потерь.

Следует выяснить, осуществляет ли провайдер резервное копирование ваших данных, и если осуществляет, то как и куда. А лучше позаботиться о резервном



А. Аксенов



Е. Богданчиков



С. Халяпин



К. Дмитриев



А. Саванович



В. Клявин



Д. Горяченков



М. Паршин



Ю. Самойлов



И. Хала

копировании самому. Тем более что это один из способов борьбы с атаками шифровальщиков, число которых, по данным компании Veeam Software, за время пандемии выросло в семь раз. «Бэкап – последний оплот защиты», – напомнил Владимир Клявин, региональный директор Veeam Software по России, СНГ, Грузии и Украине. Зачастую созданию бэкапов не уделяется достаточного внимания, однако, как предостерег эксперт, устаревшие решения для резервного копирования, не успевающие за стремительным развитием платформ, не смогут защитить бизнес.

По данным Veeam, сейчас 32% пользователей осуществляют резервное копирование с помощью локальных инструментов, но через два года их доля сократится до 13%. Популярность набирают облачные сервисы. Доля клиентов, самостоятельно управляющих бэкапами с помощью облачных сервисов, достигнет в 2023 г. 41%, а с использованием поставщика услуг – 39%.

Кадры опять решают все

«Проблема России – дефицит кадров», – отметил руководитель отдела продаж ИТ российско-итальянской компании ДКС Денис Горяченков. Один из ведущих российских производителей электротехнической продукции, практически монополист с долей 40% на рынке металлических труб и гибких трубопроводов в Италии, имеющий 12 производственных площадок в пяти странах мира, испытывает трудности с подбором специалистов для работы на своем заводе в Твери. Хотя именно в этом городе с открытия 20 лет назад производственно-складского комплекса и выпуска гофрированных труб для электропроводки началась история компании.

Дефицит кадров для отрасли ЦОДов отметил и Константин Королев, директор по развитию отраслевых инициатив АНО «Координационный совет по ЦОДам и облачным технологиям». По данным опроса, проведенного АНО КС ЦОД, лишь в 12% ЦОДов штат обслуживающего персонала укомплектован полностью. Эта проблема общемировая – индустрия ЦОДов развивается столь быстро, что система найма, обучения и переобучения специалистов просто не выдерживает такого темпа. Обеспечение притока и подготовки кадров для отрасли – одно из основных направлений работы АНО КС ЦОД.

Государство и ЦОДы

Нужна ли отрасли ЦОДов поддержка со стороны государства, а если да, то какая?

«В течение года мы работали над пакетом мер поддержки и готовы обсуждать корректировку условий и правил льготного кредитования», – заявил на панельной дискуссии «Развитие рынка ЦОДов. От чего зависит?» Максим Паршин, заместитель министра цифрового развития, связи и коммуникаций РФ. Льготы – это хорошо, но многое зависит от условий их предоставления. Если льготное кредитование будет увязываться с покупкой недостаточно надежного отечественного оборудования, то такие условия, по мнению А. Аксенова, дата-центрам, заботящимся об обеспечении бесперебойной работы клиентов, не подойдут. Также глава IXcellerate отметил важность равного доступа к льготам для всех участников рынка.

Мысль о том, что господдержка – вещь обоюдоострая, выразил и Е. Богданчиков: «Если появится объект, который можно поддерживать, то появится и возможность его регулировать. Рынок ЦОДов рос за счет того, что участие государства в индустрии было минимальным. Не мешайте работать, и мы все сделаем в лучшем виде». Сегодня же получение всевозможных разрешений и согласований сильно тормозит развитие ЦОДов. «Мы строим и запускаем ЦОД быстрее, чем согласовываем фасад, хотя находимся в промзоне, где никого больше нет», – посетовал исполнительный директор DataPro.

Вместе с тем государственные заказчики создают значительный спрос, который является драйвером рынка. «Рынок находится на подъеме, и мне совестно просить дополнительные преференции и льготы у министерства. Есть много направлений в ИТ, где ситуация выглядит не так хорошо, как у нас», – признал первый заместитель генерального директора компании «Ростелеком-ЦОД» Юрий Самойлов.

«Запрет строительства государственных ЦОДов – стопроцентное попадание в поддержку отрасли. Это лучшая мера, которую можно придумать», – считает генеральный директор 3data Илья Хала. Вопрос о запрете строительства новых дата-центров за счет бюджетных средств на тот момент обсуждался на самом высоком уровне и в итоге был включен во «второй пакет мер поддержки ИТ-отрасли».

Николай Носов



НОВОСТИ АНО КС ЦОД

СЕНТЯБРЬ 2021

Меры поддержки отрасли ЦОДов приняты правительством РФ

Премьер-министр РФ Михаил Мишустин утвердил план мероприятий («дорожную карту») создания дополнительных условий для развития ИТ-отрасли, который часто называют вторым пакетом мер поддержки ИТ-отрасли. АНО КС ЦОД активно участвовала в проработке вошедших в этот пакет мер, связанных с развитием отрасли центров обработки данных. Этот документ предлагает фактически запретить госорганизациям строить дата-центры за бюджетные средства. Также предусматриваются предоставление по кадастровой стоимости земельных участков для коммерческих ЦОДов и упрощение процедуры их подключения к электросетям.

ОКТАБРЬ 2021

Прошел третий тренинг АНО КС ЦОД

АНО КС ЦОД провела в Москве очередной тренинг «Построение ЦОДа». В рамках насыщенной программы обучения, занявшей три полных дня, рассматривались все аспекты планирования, бюджетирования, построения и эксплуатации ЦОДов. На протяжении всего тренинга 30 слушателей изучали не только теоретические аспекты, но и приводимые лекторами практические примеры из своего богатого опыта. Завершающие дискуссии по широкому кругу вопросов отразили живой интерес и слушателей, и самих лекторов к затронутым темам. Следующий тренинг назначен на I квартал 2022 г. О точных сроках будет объявлено на сайтах apo-dcc.ru и iksmmedia.ru.

НОВОСТИ ОТРАСЛИ

Облака VK в ЦОДах Казахстана

На территории Республики Казахстан начнет работать облачная платформа VK Cloud Solutions (ранее – Mail.ru Cloud Solutions, MCS). Партнером «VK Цифровые Технологии» стала казахстанская компания QazCloud, владеющая дата-центрами и технологическими компетенциями в развитии цифровых услуг на территории Казахстана. Казахстанские компании получат доступ к облачным сервисам MCS, размещенным в ЦОДах QazCloud, с соблюдением требований местного законодательства в отношении локализации данных.

QazCloud открыл новый дата-центр

Казахстанский инфраструктурный провайдер QazCloud ввел в эксплуатацию ЦОД в г. Косшы Акмолинской области (в 20 км от Нур-Султана). Его общая площадь – 259 кв. м, в машзале установлено 100 стоек. Модульный дата-центр спроектирован

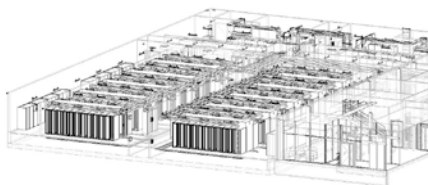


Источник: profit.kz

в соответствии с требованиями надежности дата-центров уровня Tier II (обеспечивается бесперебойная работа ЦОДа в течение 99,749% времени).

ВЭБ поддержит проект создания ЦОДа в Приморье

На Восточном экономическом форуме государственная корпорация развития ВЭБ.РФ, Корпорация развития Дальнего Востока и Арктики и дата-центр Key Point



Источник: Key Point

заключили соглашение о сотрудничестве в реализации проекта создания дата-центра уровня Tier III на территории опережающего развития «Надеждинская» (Приморский край). Общая стоимость проекта оценивается в 1,8 млрд руб.

Yandex.Cloud выходит на европейский рынок

До конца 2022 г. облачная платформа Yandex.Cloud откроет нескольких зон доступности в Европе. Первый «облачный регион» за пределами России разместится в Германии. Платформа будет развернута на базе мощностей коммерческого оператора дата-центров, соответствующего немецким, общеевропейским и мировым стандартам. Для реализации проекта будет использовано серверное и сетевое оборудование, разработанное и произведенное при участии и под контролем специалистов «Яндекса». На первом этапе для работы в европейском регионе запланирована поставка и установка 864 серверов нового поколения. Российский и европейский регионы будут связаны таким образом, чтобы сохранить отказоустойчивость сервисов и упростить компаниям одновременное использование обеих локаций. Защита данных, расположенных на серверах в европейской юрисдикции, будет регулироваться местными законодательными и нормативными актами.

НЦСД планирует построить ЦОД в Дубне

Экспертный совет по технико-внедренческому особым экономическим зонам

при правительстве Московской области одобрил бизнес-планы трех компаний, которые выбрали местом реализации своих проектов территорию ОЭЗ в Дубне. Самый крупный из представленных экспертному совету – проект компании «Надежный Цифровой Сервис Данных», которая инвестирует в него около 5 млрд руб. и создаст 70 рабочих мест. Проект предусматривает разработку технологий и систем хранения, обработки и передачи данных, а также разработку и внедрение сопутствующего ПО. Для реализации поставленных целей компания намерена построить современный высокотехнологичный ЦОД площадью 20 тыс. кв. м.

«Ростелеком-ЦОД» открывает новый дата-центр Tier III в Москве

Компания «Ростелеком-ЦОД» запускает в эксплуатацию новый ЦОД NORD-6. Объект общей площадью 3 тыс. кв. м и мощностью 5 МВт расположен в Москве по адресу Коровинское шоссе, 37. В двух машинных залах размещается 207 стоек. Главная особенность проекта – группа стоек с повышенной мощностью 20 кВт.



Источник: «Ростелеком-ЦОД»

«Яндекс», ЛАНИТ, Gigabyte и ВТБ построят под Рязанью завод по производству серверов

Совместное предприятие, созданное «Яндексом», ГК ЛАНИТ, производителем компьютерной техники Gigabyte и банком ВТБ, приступило к строительству завода по производству серверного оборудования. Производственный комплекс расположится на территории индустриального парка «Рязанский» и будет выпускать оборудование под торговой маркой Opreyard: серверы, системы хранения данных, шлюзы и компоненты «умных» устройств. Ожидается, что первый сервер завод поставит на рынок до конца 2022 г.

«Ростелеком» откроет в Заполярье первый ЦОД в Арктике

«Ростелеком» построит в Мурманской области первый в российской Арктике региональный центр обработки данных, запуск которого планируется уже в июле 2022 г. Об этом сообщил директор макрорегионального филиала «Северо-Запад» ПАО «Ростелеком» Александр Логинов. К работам планируется приступить в конце текущего года или в начале 2022-го.

ЦОД – отечественный на 70%. Когда?

Александр Барсков

Отечественные производители активно наращивают выпуск решений для инженерной инфраструктуры ЦОДов. Однако ведущие дата-центры не спешат использовать их продукцию.



На организованном «ИКС-Медиа» международном форуме «ЦОД» впервые за 16 лет его проведения целый конференционный поток был посвящен отечественным решениям. Немало стендов с российскими продуктами было развернуто на выставке форума. Интерес российских производителей к быстрорастущей индустрии ЦОДов очевиден.

Выступая на форуме, Максим Паршин, заместитель министра цифрового развития, связи и коммуникаций РФ, рассказал о запущенной государством программе льготного кредитования с целью поддержки отечественных производителей. Компании, которые при построении ЦОДов используют не менее 70% отечественных решений, могут рассчитывать на кредит по ставке 1–5%. Недополученные банками доходы – а в программе уже участвует 18 ведущих финансовых учреждений – будет компенсировать государство.

Ассортимент на сегодня

Чтобы понять, насколько реально достичь названных 70%, давайте на примере участников форума «ЦОД» проанализируем, что сегодня предлагают российские компании для инженерной инфраструктуры дата-центров.

Компания ДКС с основной производственной площадкой в Твери и оборотом 400 млн евро, по заверению ее представителей, входит в число крупнейших производителей кабеленесущих систем и низковольтного оборудования в России и Европе. Как заявил Денис Горяченков, руководитель отдела продаж ИТ этой компании, для ЦОДов она «предлагает практически все, кроме климатики». В портфеле ДКС – широкий ассортимент кабельных каналов и систем, корпусное оборудование, современные ИБП, в том числе большой мощности (которые производятся в Италии). На форуме компания демонстрировала мини-ЦОД Net One – готовое решение для замены серверных комнат (рис. 1).

Группа компаний ИЕК под брендом ИТК выпускает самую разнообразную кабельную продукцию (в том числе медножильные и оптические системы, рис. 2), а также блоки распределения питания (PDU), шкафы и аксессуары для ЦОДов. Планы компании, о которых сообщил Артем Шарапов, руководитель направления технической поддержки ИТК, весьма амбициозны. Уже в ближайшее время бренд ИТК намеревается наладить производство систем ИБП и кондиционеров (в основном по OEM-модели). Кроме того, ГК ИЕК принадлежит MasterScada – одна из лидирующих на российском рынке систем автоматизации.

Компания C3 Solutions, изначально сфокусировавшая свою деятельность на рынке ЦОДов,



◀ Рис. 1. Мини-ЦОД Net One производства ДКС

наверное, наиболее на нем известна. Она изготавливает монтажные шкафы, PDU, лотки и готовые решения, в том числе микроЦОДы (рис. 3). Компания активно заключает партнерские OEM-соглашения и под своим брендом предлагает комплексные решения. Накануне форума было объявлено о слиянии C3 Solutions с другим отечественным производителем – компанией «Новые Технологии», которая выпускает всевозможные шкафы, открытые и закрытые, настенные и напольные, защищенные, климатические. Кроме того, компания «Новые Технологии» предлагает системы автоматизации гражданских и производственных объектов, решения для «умных» городов и зданий.

На рынок решений для ЦОДов выходят и новые игроки, как правило, ранее работавшие в других сегментах. Так, компания «ОМП-Инжиниринг» представила на форуме свою экспертизу в области проектирования, производства и монтажа инженерных систем тепло/холодоснабжения (холодильных центров, тепловых пунктов, насосных станций). Компания практикует цеховое изготовление элементов трубопроводов по 3D-модели с последующей сборкой на объекте (сборка «лего», рис. 4). По сути, это решения высокой заводской готовно-



◀ Рис. 2. Кассета волоконно-оптической кабельной системы производства ИТК



Рис. 3. МикроЦОД производства С3 Solutions ▶

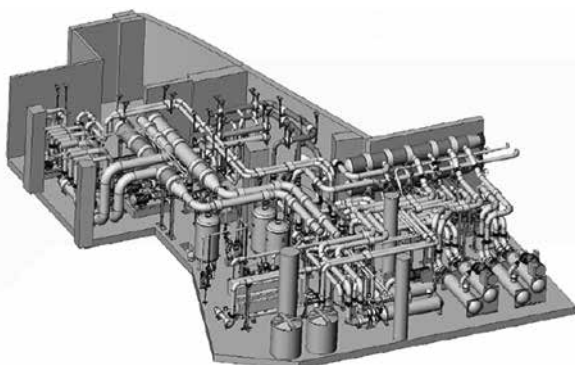
сти, которые позволяют существенно сократить срок создания объектов.

Еще одно новое имя для цодостроителей – компания ПСМ. По данным, опубликованным на ее сайте, компания занимает первое место среди российских производителей дизель-генераторов с долей рынка 25%. Для ЦОДов она проектирует и выпускает системы гарантированного энергоснабжения, включая дизельные электростанции, ИБП, распределительные устройства, контейнерные топливозапасники. Завод ПСМ (рис. 5) работает с такими мировыми брендами, как Mitsubishi, Cummins, Perkins, Stamford, Leroy Somer, Schneider Electric, Delta Electronics и др.

Свои решения представили на форуме и другие отечественные компании:

- ГК «Пожтехника» – комплексные системы пожарной безопасности;
- ЦРИ «Импульс» – источники бесперебойного питания;
- «Парус электро» – силовую преобразовательную технику, в том числе ИБП (под маркой «Связь инжиниринг»);

Рис. 4. 3D-модель и подготовка трубной обвязки на заводе «ОМП-Инжиниринг» ▼



- «Веза» – вентиляторы, теплообменники, кондиционеры и другую климатическую технику (по данным компании, она является единственным в России предприятием полного технологического цикла производства указанных изделий);
- METAENERGY – широкий спектр электрооборудования, распределительных систем и комплектующих для нужд электроснабжения, в том числе для низковольтного оборудования, для среднего и высокого напряжения.

Как видим, перечень заявленных решений весьма внушительен. Он охватывает все основные подсистемы инженерной инфраструктуры ЦОДов. Но насколько велик интерес к отечественной продукции у операторов ЦОДов?

Вопросы к качеству

Оператор сети ЦОДов Zdata, по словам его генерального директора Ильи Халы, при покупке оборудования руководствуется не его происхождением, а эффективностью. Ключевых показателей три: качество, цена и сроки поставки.

«У локализованного оборудования очевидные преимущества в сроках поставки, в также в отсутствии рисков трансграничных перевозок и таможенных процедур. Цена бывает ниже. Но к качеству есть вопросы, – рассказывает И. Хала. – То, что научились делать качественно, мы с радостью покупаем». К такому оборудованию руководитель Zdata относит серверные шкафы («даже если шильдик иностранный, шкафы часто производят в РФ»), блоки распределения питания («много берем российских PDU»), кабельные лотки.

«Но это простые позиции, – продолжает И. Хала. – Что касается сложного оборудования, то здесь ситуация иная: кондиционеры – это 100% импорт, ДГУ и ИБП – что-то в России есть, но качество нас пока не устраивает. Будет расти качество, конечно, будем брать российское. Это удобнее».

«Мы следуем концепции устойчивого развития, а один из ее блоков – поддержка местных поставщиков. Этот тренд наблюдается во всем мире. И мы хотели бы закупать большую часть решений в России. Но не любой ценой», – фор-



◀ Рис. 5. Завод металлоконструкций ПСМ

мулирует свою позицию Андрей Аксенов, генеральный директор компании IXcellerate, входящей в топ-3 российских операторов коммерческих ЦОДов.

По его словам, никакие льготные кредиты не заставят его компанию закупать продукцию, которая не проверена «в боевых условиях». «Мы не готовы тестировать оборудование на наших крупных клиентах, среди которых, в частности, банки и поставщики облачных сервисов. Если оно окажется ненадежным, то от этого могут пострадать тысячи и миллионы людей – вы подойдете к банкомату, а он не работает», – продолжает он.

Руководитель IXcellerate тоже указывает на серьезные преимущества отечественных решений в плане сроков доставки. «Одно из ограничений сегодня – долгий срок поставки. Из Европы, США, Китая оборудование сейчас идет по два-три месяца. Очень неприятная ситуация, – говорит он. – Россия сильно продвинулась в сервисе, проектировании и построении ЦОДов. Но в производстве есть фундаментальные проблемы, которые за год-два не решить».

Еще один представитель «большой тройки» операторов ЦОДов, компания DataPro использует некоторое отечественное оборудование, но, как заявил ее исполнительный директор Евгений Богданчиков, «ни по одной линейке [основного] оборудования [среди отечественных производителей] не видим достойных конкурентов ни западным, ни даже азиатским производителям».

«Первые бенефициары роста рынка ЦОДов – зарубежные производители. Поэтому важно, чтобы государство стимулировало их к локализации производства», – добавил он.

Что будет

Три российские компании – ДКС, ИТК и С3 Solutions – заявили на форуме «ЦОД» о том, что в ближайшее время будут готовы представить полные решения, охватывающие все основные инженерные системы дата-центра. Причем Максим Кыркунов, генеральный директор С3 Solutions, объявил о намерении пойти по пути формирования зонтичного бренда, собрать под него отечественных производителей систем для ЦОДов и создать поставщика мирового уровня и масштаба.

Подобные намерения можно только приветствовать. Но, при всем масштабе российского рынка ЦОДов, будет ли его емкость достаточной, чтобы обеспечить заказами сразу нескольких отечественных «шнайдеров»? Ведь даже на глобальном рынке число поставщиков полных решений для ЦОДов можно пересчитать по пальцам одной руки. Возможно, правильнее будет сформировать единого отечественного поставщика, например, по модели, предложенной С3 Solutions. Однако амбиции каждой отдельной компании могут сильно затруднить такой проект. Что, собственно, мы наблюдали на рынке телекоммуникационной продукции, где отечественный «хуавей» так и не появился.

Как заявил М. Паршин, пакет на сумму более 40 млрд руб. для льготного кредитования проектов на основе отечественных продуктов уже сформирован. Несколько запросов от цодостроителей поступило, они рассматриваются и находятся «в высокой степени готовности». Но пока такого кредита никто не получил. Как только это произойдет, надеемся, мы узнаем, кто же рискнул построить «на 70% отечественный» ЦОД. ИКС

Системы хранения данных: сделано в России

Дисковые массивы отечественного производства уже заявили о себе как о перспективном конкуренте общепризнанных лидеров рынка СХД.

Дмитрий Грачев, ведущий инженер отдела «Инфраструктура», «ЛАНИТ-Интеграция» (ГК ЛАНИТ)

За последние три–пять лет российские компании столкнулись с множеством вызовов: с изменениями во внешнеполитической обстановке, пандемией COVID-19 и переходом сотрудников на удаленную работу. Все это наложило серьезный отпечаток на то, как теперь бизнесу необходимо подходить к информационным технологиям и цифровой трансформации.

В процессе импортозамещения отечественные компании, у которых доля участия государства в уставном капитале составляет не менее 50%, активно рассматривают отечественные решения как альтернативу иностранному оборудованию и ПО. Полагаясь на свой прошлый и текущий опыт работы с государственными заказчиками, расскажем об отечественных системах хранения данных, которые занесены в реестры российского оборудования и ПО и предназначены для выполнения задач разных типов.

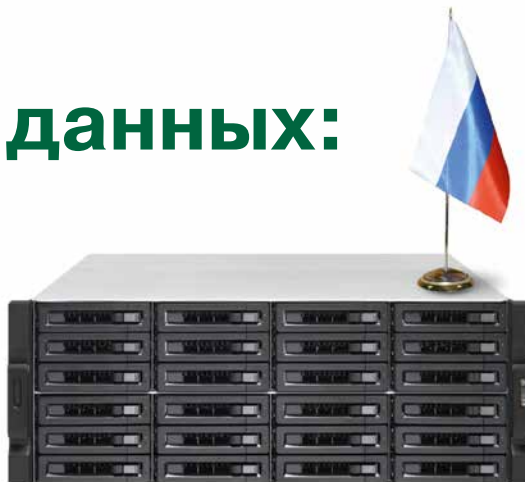
Виды систем хранения данных

Сегодня все системы хранения данных по их назначению и уровню производительности можно условно разделить на следующие категории:

- СХД общего назначения;
- СХД all-flash для бизнес-критичных данных;
- массивы для хранения архивных данных и резервных копий;
- программно определяемые СХД.

СХД общего назначения

К системам хранения общего назначения относят дисковые массивы, которые в равной степени подходят для хранения и данных бизнес-критичных информационных систем, и данных с менее строгими требованиями, например, пользовательских данных сотрудников компании и резервных копий. Критичные приложения требуют от СХД высокой производительности,



сти, следовательно, поддержки флеш-накопителей и быстрых жестких дисков. Важна и работа с современными протоколами передачи данных. Простой информационной системы может привести к серьезным убыткам, а значит, необходимо обеспечить резервирование всех компонентов массивов. Это относится к подключению к каналам связи, накопителям, блокам питания и контроллерам – вычислительным узлам СХД. Эффективное хранение файловых данных и резервных копий подразумевает поддержку вместительных механических дисков и возможность масштабирования до больших объемов хранения. Полезны функции автоматического переноса данных между уровнями хранения, содержащими накопители разной производительности, создание мгновенных снимков томов, синхронная и асинхронная репликация, дедупликация данных.

Примером российского дискового массива общего назначения может служить TATLIN. UNIFIED от компании Yadro. Устройство хранения поддерживает одновременную работу двух контроллеров со всеми современными типами накопителей. Подключение к сети передачи данных может осуществляться по протоколам FC 32/16 Gb и Ethernet 10/25 Gb. Благодаря технологии Erasure coding и резервированию основных компонентов надежность СХД достаточно высока. Массив способен работать со всеми популярными операционными системами и системами виртуализации, а технология тонкого выделения емкости помогает экономить дисковые ресурсы. Стоит отметить поддержку флеш-накопителей NVMe – это современный протокол работы с флеш-памятью, позволяющий существенно повысить производительность. Большинство ИТ-специалистов сходятся во мнении, что за такими накопителями будущее систем хранения.

Еще один представитель российских систем хранения – «Аэродиск Восток Э12», СХД общего назначения на основе процессоров «Эльбрус». Массив имеет широкие возможности масштабирования благодаря поддержке до восьми контроллеров. Обеспечивается подключение по FC и Ethernet, а также файловый доступ к данным по протоколам NFS и CIFS. Функционал включает возможность создания мгновенных снимков томов и их миграцию между контроллерами системы в режиме онлайн.

СХД all-flash для бизнес-критичных данных

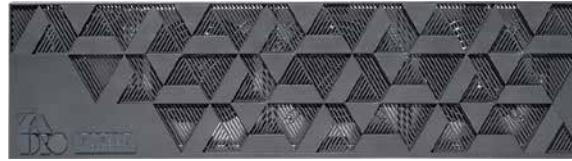
All-flash СХД – это устройства, оптимизированные для использования только флеш-накопителей. Из-за своей высокой стоимости они применяются исключительно для критичных задач. Массивы all-flash обладают самой высокой производительностью из всех доступных сегодня систем хранения. Как и в случае массивов общего назначения, к их надежности предъявляются высокие требования. Однако с распространением технологии NVMe и общей тенденцией к удешевлению флеш-технологий такие массивы становятся все популярнее.

На данный момент полноценных all-flash решений среди российских СХД нет. Компании указывают, что могут поставить массивы в конфигурации только с флеш-накопителями, но называть подобные СХД all-flash некорректно. У массивов, не предназначенных для работы с механическими дисками, обычно отсутствует часть программного кода, что дополнительно увеличивает их производительность. All-NVMe-решения работают только с протоколом NVMe и не поддерживают SCSI, который был разработан именно для классических жестких дисков. Вполне вероятно, дальнейшая популяризация отечественных решений изменит ситуацию в лучшую сторону.

СХД для архивных данных

Хранение архивных данных предполагает поддержку массива дисков большого объема с относительно невысокой производительностью. Часто для таких решений используются полки высокой плотности, содержащие до 40–80 накопителей. Полное резервирование всех компонентов не всегда критично, поэтому архивные СХД могут включать всего один контроллер. Поскольку системы резервного копирования и архивации данных могут работать по файловым протоколам (CIFS, NFS), поддержка таковых является полезным дополнением.

Для задач архивного хранения хорошо подходит, например, решение SIRIUS 8000 от компа-



◀ СХД Yadro TATLIN.UNIFIED

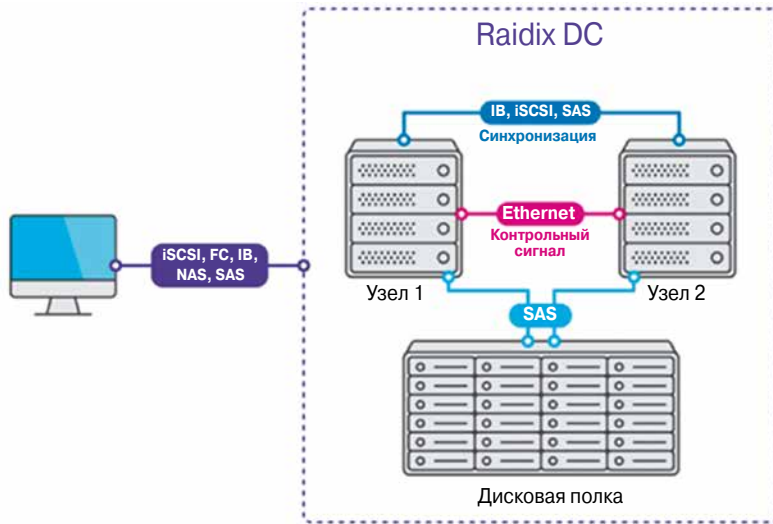


◀ СХД «Аэродиск Восток Э12»

нии «Промобит» (бренд Bitblaze). Это распределенная горизонтально масштабируемая СХД с поддержкой до 5800 дисков и полок высокой плотности на 56 накопителей формата LFF (3,5 дюйма). Горизонтальное масштабирование подразумевает, что при добавлении дисков к системе будут добавляться вычислительные узлы – контроллеры. Таким образом, масштабирование выполняется практически линейно, т.е. с ростом объема растет и производительность. Массив работает под управлением распределенной файловой системы Bitblaze KFS, состоит из узлов хранения и управления, обеспечивающих доступ к данным. Доступ осуществляется по блочным протоколам FC и iSCSI, а также по файловому протоколу NFS.

Структура СХД Bitblaze SIRIUS 8000 от компании «Промобит» ▼





▲ Двухконтрольный режим работы СХД от «Рэйдикс»

Программно определяемые СХД

Программно определяемая СХД – это программное обеспечение, которое устанавливается на серверы общего назначения, объединяя их в кластер и превращая в гибкий распределенный массив хранения данных. Отказоустойчивость таких решений часто строится на возможности потери целых узлов кластера. Важное преимущество состоит в том, что требования к используемым серверам достаточно либеральны. Компания может организовать СХД путем установки ПО на российские серверы.

Представитель российских программно определяемых СХД – решение компании «Рэйдикс». Оно позволяет построить универсальный дисковый массив в виде отказоустойчивого кластера с поддержкой блочных протоколов доступа к данным FC, iSCSI, SAS, а также файло-

вых NFS, CIFS и FTP. Поддерживается множество вариантов уровней RAID для защиты данных, а также репликация между СХД для обеспечения непрерывности бизнеса. Взаимодействие узлов массива между собой осуществляется по протоколам InfiniBand и iSCSI.

Основные тренды развития российских СХД

От системы хранения зависят устойчивость и непрерывность бизнеса в целом. Проведение аудита, грамотные сайзинг и подбор решения помогут сэкономить средства компании и время сотрудников. В настоящее время на рынке присутствует множество разнообразных СХД от отечественных производителей, и текущая политическая ситуация указывает на то, что со временем их будет становиться больше.

Объем оборудования, поставляемого государственным компаниям, стабильно высокий, а значит, эта часть рынка всегда будет интересна как производителям, так и компаниям-интеграторам. Когда отечественные вендоры только начали процесс импортозамещения, было трудно представить, что российское оборудование будет действительно интересно заказчикам.

Сегодня отечественные решения – неотъемлемая часть жизни государственных организаций. В процессе импортозамещения системы хранения данных совершенствуются и постепенно становятся хорошей альтернативой зарубежным системам. Вполне вероятно, что в будущем дисковые массивы российского производства заинтересуют и компании, не входящие в круг тех, кто обязан выполнять требования регуляторов. **ИКС**

ИКС-Медиа на YouTube

ИКС Медиа

ГЛАВНАЯ ВИДЕО ПЛЕЙЛИСТЫ КАНАЛЫ О КАНАЛЕ

Вы подписаны

16+

Загрузки ВОСПРОИЗВЕСТИ ВСЕ

УПОРЯДОЧИТЬ

Дискуссия «ЦОД-2020: новые вызовы и...

Трансформация бизнеса с помощью облачных...

Российские высокопроизводительные...

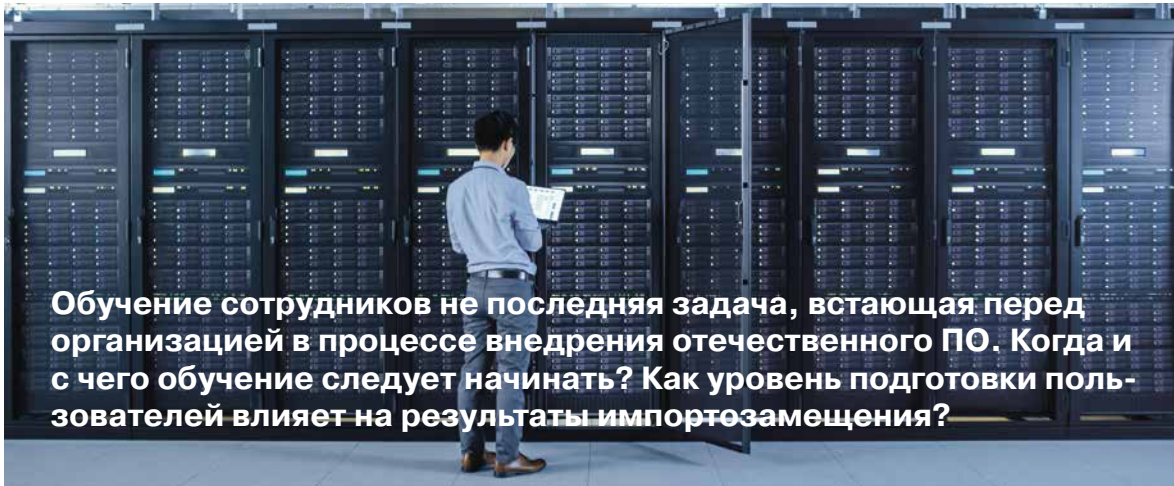
Прогноз для ЦОД от Juniper: облачно (с...

DevOps: автоматизация решает не все. Станисла...

Развертывание веб-сайта в облаке...

Опубликованы подборки выступлений на конференциях «ЦОД-2020», «ЦОД. Регион», церемонии награждения DC Awards 2020 и т.д.

Импортозамещение: не забудьте об обучении персонала



**Георгий
Кашин,**
руководитель
проектов,
«ЛАНИТ-
Интеграция»
(ГК ЛАНИТ)

Обучение сотрудников не последняя задача, встающая перед организацией в процессе внедрения отечественного ПО. Когда и с чего обучение следует начинать? Как уровень подготовки пользователей влияет на результаты импортозамещения?

Российским компаниям приходится все больше погружаться в тематику импортозамещения. Поскольку разнообразие используемого ПО огромно и учесть все нюансы практически невозможно, мы не будем детально рассматривать техническую сторону, а остановимся на операционных системах (ОС) и пакетах офисного ПО.

Особенности перехода на российское ПО

В процессе использования отечественного ПО у рядовых сотрудников и ИТ-специалистов проблем возникает не очень много, но все они существенны.

1. Страх перед изменениями. Будем честны, даже другое расположение часто используемой кнопки при очередном обновлении приложения у каждого десятого пользователя вызывает легкое раздражение. Поэтому реакция на полное изменение операционной системы или офисного ПО вполне понятна. Такая же ситуация с администраторами ОС: ни один обучающий курс не заменит многолетний опыт эксплуатации знакомых продуктов.

2. Уровень технологической конкурентоспособности. Здесь речь идет не о субъективных предпочтениях, а о фактических преимуществах зарубежных продуктов. Рассматривая ОС и пакеты офисного ПО, несложно назвать преимущества зарубежных продуктов перед рос-

сийскими. Так, ОС будут отличаться как количеством функциональных возможностей, доступностью информации о работе со всеми реализованными технологиями, так и уровнем технологичности использованных решений, протоколов и т.д. А в случае с офисными пакетами различия заключаются в количестве реализованных функций и поддержке макросов в Excel, функциональных возможностях Outlook с точки зрения кастомизации и автоматизации, поддержке расширений для многочисленных коммуникационных программ, широких возможностях аналитики и генерации отчетов в Access.

3. Ограниченность целевой аудитории. На законодательном уровне, согласно приказу Минкомсвязи России от 20.09.2018 № 486, вопрос импортозамещения касается только госучреждений, госпредприятий, учреждений и предприятий с государственным участием 50% и более, а это существенно ограничивает целевую аудиторию.

4. Маркетинг. Есть распространенное мнение: для того чтобы продукт был интересен рынку, его достаточно сделать качественным. Однако это далеко не так. На полках в магазинах по-прежнему не представлены российские ноутбуки с операционными системами отечественных производителей, российские SaaS- и PaaS-платформы пока нельзя сравнивать по объему услуг и качеству поддержки с платформами AWS, Microsoft Azure и Google, хотя стоят они столько

же. Российские разработчики для выстраивания своих приложений предпочитают зарубежные свободно распространяемые дистрибутивы ОС Linux, зарекомендовавшие себя на мировом рынке. Поэтому тиражирование опыта и практик – неотъемлемая часть развития внутреннего продукта для постепенного устранения зависимости от зарубежных предложений.

ПО Linux как первая ступень в изучении российского ПО

Отправной точкой в обучении ИТ-специалистов работе с российскими продуктами должно быть знакомство с любыми ОС семейства Linux и их администрирование. Это обусловлено тем, что российские ОС являются деривативами свободно распространяемых зарубежных ОС, а операционная система – базовый компонент практически любого решения. Очевидно, что начинать стоит именно с изучения ОС семейства Linux. Каких-либо предпочтений здесь нет, однако отметим, что IBM недавно купила компанию Red Hat, а вместе с ней CentOS, и стратегия развития продукта изменилась. Актуальными для российских специалистов остаются системы Debian и SuSE. И уже после приобретения опыта работы с ОС на базе GNU/Linux можно говорить о средствах автоматизации, построенных на базе указанных ОС, и разворачивании решений для корпоративных задач.

То же самое относится к рядовым пользователям. Начинать стоит со знакомства и выполнения базовых задач, но лучше сразу использовать те российские ОС и программные средства, на которые планируется переходить, поскольку различия в интерфейсах и функциональных возможностях между российскими ОС могут быть весьма существенными, и эти различия также будут вызывать затруднения в работе.



Когда нужно начинать обучать сотрудников правильному использованию российских продуктов? Ответ очевиден – чем раньше, тем лучше. Поскольку большинство российских ОС построены на базе ядра GNU/Linux, подготовку ИТ-специалистов целесообразно начинать именно со знакомства с независимыми

дистрибутивами, причем делать это можно и нужно за полгода и более до старта процесса импортозамещения в компании. Тому есть ряд причин.

- Обучение развивает и расширяет кругозор сотрудников компании.
- Понимая, как работают технологии, ИТ-специалисты могут стать агентами изменений в ходе проектов импортозамещения.
- Опытные ИТ-специалисты смогут общаться с интеграторами и участвовать в принятии решений об использовании того или иного функционала.
- Инженеры на стороне заказчика смогут развешивать внедренные решения после импортозамещения.
- Специалисты смогут самостоятельно внедрять бесплатные enterprise-решения на базе российских ОС.

Значение подготовки персонала в проекте импортозамещения

Несколько лет назад наша команда одновременно вела проекты запуска российского ПО в компании нефтегазового сектора и на производстве двигателей. ИТ-специалисты первой компании практически не имели опыта работы с продуктами и ОС на базе GNU/Linux, а ИТ-специалисты второй уже прошли обучение по Debian и имели опыт разворачивания и тестирования решений в сфере автоматизации. ИТ-специалисты нефтегазовой компании сталкивались с трудностями на всех этапах проекта, начиная от чтения пояснительной записки до поддержки пилотной группы пользователей в ходе тестовой эксплуатации. Неосведомленность сотрудников замедляла работу и усложняла взаимодействие. В то же время ИТ-специалисты второй компании сформулировали точные требования к проекту, не имели проблем при согласовании проектной документации, принимали активное участие в обсуждениях, а при тестировании одного из решений внесли существенный вклад в автоматизацию разворачивания нестандартного ПО.

Эти проекты показали, что обучение рядовых сотрудников также требует внимания. Осуществив проекты перевода на российское ПО для 12 тыс. АРМ и десятков инфраструктурных ИТ-систем, наша команда поняла, что для успешной реализации импортозамещения нельзя пропускать этап пилотного внедрения и тестовой эксплуатации на «живых» задачах. Пропустив этот шаг, не испытав конкретный дистрибутив ОС или ПО и делая выбор только на основании открытых данных и документации, заказчики нередко обрекают себя на затраты на внедрение дополнительных решений,

Производитель	Microsoft	«Базальт СПО»	НТЦ ИТ РОСА	«Новые облачные технологии» («МойОфис»)	«Новые коммунационные технологии» («Р7 Офис»)
Расписание курсов	Не менее одного курса в неделю по основным продуктам в десятках УЦ*	Не более двух раз в месяц по каждому курсу в трех УЦ	Три партнерских УЦ, нет открытого расписания	На сайте производителя информация отсутствует	Нет открытого расписания, в двух УЦ
Специальная сертификация преподавателя	Да	Неизвестно	Неизвестно	Неизвестно	Неизвестно
Наличие у преподавателя сертификата, подтверждающего знания курса	Да	Неизвестно	Неизвестно	Неизвестно	Неизвестно
Многоуровневая система сертификации для повышения квалификации	Да	Нет	Нет	Нет	Нет
Объем данных о продуктах в БЗ (субъективно)	Огромный	Средний	Небольшой	Небольшой	Средний
Бесплатные обучающие материалы по продуктам	Да	Нет	Нет	Нет	Да

*УЦ – учебный центр

усложнение бизнес-процессов или даже остановку проектов. Пилотные проекты и тестовая эксплуатация – это тот момент, когда нужно начать вовлекать рядовых пользователей в процесс обучения.

Во время подготовки проектов интеграторы не только пишут инструкции, но и организуют семинары, лекции, делают видеозаписи, обучающие базовым операциям при работе с АРМ и основным ПО. По результатам пилотных проектов иногда создаются стенды, а отдельные пользователи привлекаются к выполнению базовых бизнес-задач на импортозамещающих АРМ.

Стандарты для подготовки специалистов и образовательная база

Наша команда провела сравнительный анализ обучающих курсов, предлагаемых популярными российскими и зарубежными разработчиками ОС и офисного ПО. Анализ выявил низкую востребованность курсов по администрированию российских ОС и офисных продуктов у ИТ-специалистов. Это косвенно указывает на невысокие показатели эффективности импортозамещения. При детальном рассмотрении расписаний обучающих курсов прослеживается разнородность их состава, отсутствие четких стандартов в подходах к обучению. Однако в этом направлении мы видим и прогресс – от полного отсутствия обучающих курсов и материалов к структурированной подаче информации и партнерству с большим числом учебных центров.

Стоит отметить, что у Microsoft тренеры получают не только сертификат, подтверждающий знание собственно курса, но и специальный сертификат преподавателя, удостоверяющий, что он способен качественно донести материал до слушателей.

Перспективы импортозамещения в России

Импортозамещение только набирает обороты, внедрение российских продуктов пока вызывает сложности из-за непопулярности инфраструктурного ПО и операционных систем. Крупные зарубежные вендоры вырабатывали стандарты и подходы к обучению специалистов в области управления и администрирования их систем десятилетиями, российские же разработчики только начинают формировать такую базу, и каждый из них идет в этом своим путем. По открытой информации о реализованных проектах и согласно данным Минпромторга России, продление сроков импортозамещения обусловлено не только отсутствием необходимых продуктов, но и недостаточным количеством квалифицированных ИТ-специалистов. Такая ситуация наблюдается во многих сферах, которые подпадают под действие постановления Правительства РФ от 23.03.2017 № 325, устанавливающего дополнительные требования к отечественному офисному ПО.

Текущий внешнеполитический курс и показатели эффективности импортозамещения в сфере ИКТ говорят об одном – сроки реализации проектов будут продлеваться, а это означает, что финансирование развития российских ОС и продуктов основной инфраструктуры будет продолжаться. В свою очередь, это повлечет за собой необходимость увеличить количество и повысить качество обучающих материалов и специализированных курсов. В сфере ИТ-образования механизмы те же, что и в остальном мире, – спрос рождает предложение. Как только масштабы использования российского ПО достигнут «критической массы», мы увидим кратный рост интереса и к обучению. **ИКС**

▲ Обучающие курсы зарубежных и российских разработчиков ОС и офисного ПО

ГИСы уйдут в коммерческие ЦОДы

Александр Барсков

Второй пакет мер поддержки ИТ-отрасли предлагает фактически запретить госорганизациям строить дата-центры за бюджетные средства. Он также предусматривает предоставление по кадастровой стоимости земельных участков для коммерческих ЦОДов и меры, упрощающие их подключение к электросетям.

В сентябре нынешнего года премьер-министр РФ Михаил Мишустин утвердил план мероприятий («дорожную карту») создания дополнительных условий для развития ИТ-отрасли. Предложенные в нем меры способны придать существенный дополнительный импульс развитию отрасли центров обработки данных.

К декабрю 2021 г. в нормативные документы должны быть внесены требования включить в ведомственные программы цифровой трансформации (ВПЦТ) указания на использование отечественных облачных сервисов и на отказ от создания без надлежащего обоснования инфраструктуры ЦОДов за счет бюджетных средств. Кроме того, должен быть введен запрет на создание (также без надлежащего обоснования) инфраструктуры ЦОДов для нужд органов исполнительной власти субъектов РФ.

По сути, речь идет о запрете строительства дата-центров государственными организациями за счет бюджетных средств. Такая мера, очевидно, заставит госзаказчиков обращаться к услугам коммерческих ЦОДов, что ускорит развитие этого рынка и положительно скажется на экономии государственных средств в целом, поскольку коммерческие ЦОДы строятся и эксплуатируются намного эффективнее большинства государственных объектов. Стоит отметить, что возможность создания дата-центров государственными ведомствами за счет бюджетных средств ограничена и в ряде зарубежных стран, а эффективность данного подхода с точки зрения экономии затрат на ИТ при одновременном повышении уровня сервисов подтверждена многолетней практикой.

Послужит дальнейшему развитию отрасли коммерческих ЦОДов и предложение внести в нормативные правовые акты изменения, которые обяжут субъектов РФ предоставлять земельные участки для строительства таких дата-центров без торгов по кадастровой стоимости. Это позволит уменьшить расходы ЦОДов, снизит риски прекращения права пользова-

ния имуществом ЦОДа и обеспечит лучший контроль над непрерывностью оказываемых услуг.

Наконец, подписанный премьер-министром документ затрагивает и самый больной для отрасли коммерческих ЦОДов вопрос о подключении к электросетям. Уже в ноябре 2021 г. должны быть подготовлены предложения по внесению изменений в Правила технологического присоединения к электрическим сетям, предусматривающие установление для ЦОДов отдельного порядка такого присоединения, а также оптимизацию процедуры технологического присоединения проектируемых в расчете на потребности ЦОДов подстанций к электрическим сетям высокого напряжения.

Предложенные изменения дадут ЦОДам возможность осуществлять технологическое присоединение к сетям сразу нескольких сетевых организаций, сократят время на получение и согласование технических условий у ресурсоснабжающих организаций, а также позволят оптимизировать затраты на организацию энергоснабжения ЦОДов за счет введения особого порядка технологического присоединения к электросетям.

«Все меры, касающиеся отрасли ЦОДов, активно обсуждались Минцифрой России непосредственно с отраслевым сообществом, – комментирует событие Видия Железнов, член совета АНО «Координационный совет по ЦОДам и облачным технологиям», участник Рабочей группы по разработке мер поддержки. – Для наиболее значимых мер, вошедших в финальную версию пакета, были подготовлены финансово-экономические обоснования, подтвердившие общий позитивный экономический эффект. Теперь важно реализовать предложенные меры. Необходимо разработать и внести изменения в ряд нормативных правовых документов, что потребует обсуждения с участием ответственных ведомств. АНО КС ЦОД планирует продолжить работу в данном направлении».

«Безусловно, основные системообразующие меры для рынка ЦОДов и облачных сервисов – это включение в ВПЦТ указаний на использование отечественных облачных сервисов, запрет на строительство собственных ЦОДов без надлежащего обоснования, а также запрет на строительство ЦОДов за бюджетные средства для ФОИВ», – считает Дмитрий Горкавенко, директор по развитию iKS-Consulting.

По оценкам аналитиков iKS-Consulting, сегодня в эксплуатации находятся более 30 тыс. «госстоек» с энергопотреблением 3–3,5 кВт на стойку. При этом весь объем рынка коммерческих ЦОДов в России в 2020 г. составил 48,5 тыс. стойко-мест, которые сосредоточены преимущественно (72%) в Московском регионе. «Этот разрыв – и количественный, и географический – придется “закрывать” и существующим игрокам рынка, и новым, которые теперь точно придут на этот рынок, запуская новые площадки», – продолжает Д. Горкавенко. Также следует учесть, что строительство ЦОДа от поиска площадки до пусконаладочных работ продолжается около двух лет, а при высокой утилизации (занятости) площадок в Московском регионе и спросе на стойко-места со стороны коммерческого рынка «госстойки» ставить в ближайшее время просто некуда. Кроме того, большинство игроков на рынке не имеет опыта работы с госсектором и предпочитает запускать проекты на открытый рынок, что также будет сдерживать темпы миграции «госстоек» в коммерческие ЦОДы. «Все это несколько сместит «повестку» в сторону «гособлаков», а вот далее квалифицированные операторы «гособлаков» выйдут на открытый рынок коммерческих ЦОДов, выступая потребителями или партнерами для инфраструктурных площадок», – указывает Д. Горкавенко.

Эксперт iKS-Consulting полагает, что нас ждет:

- пропорциональное укрупнение проектов – для Москвы масштаб будет начинаться с 2000 стойко-мест, для регионов – с 400 стойко-мест на проект;
- появление опорной сети ЦОДов (ранее соответствующее мероприятие было включено в паспорт Федерального проекта «Информационная инфраструктура»), тяготеющей к региональным потребителям с учетом телекоммуникационной связности как с Москвой, так и между соседними субъектами. Вероятно, появятся либо получат развитие площадки ЦОДов в Московской области, Краснодарском крае, Екатеринбурге, Красноярске, Новосибирске, ХМАО, ЯНАО, Республике Саха (Якутия), Липецке, Нижнем Новгороде, Белгороде, Уфе, Владивостоке;
- наращивание среднего энергопотребления стойки до 6–8 кВт (ранее такие стойки считались высоконагруженными) в течение следующего цикла амортизации серверного оборудования (до восьми лет с учетом вторичного рынка);
- появление модулей/залов в ЦОДах и целых площадок для госсектора со специфическими требованиями к физической безопасности;
- разработка нормативной базы в области ЦОДов и облачных сервисов, включая требования к ЦОДам и системам аккредитации поставщиков услуг.

«Учитывая утвержденные меры поддержки, мы считаем, что развитие рынка (увеличение количества стойко-мест) в 2022–2023 гг. будет опережать наши прогнозы, сделанные в соответствии с благоприятным сценарием, на 3–5% ежегодно. Но многое будет зависеть от конкретной реализации этих мер. В целом на рынке в течение пяти-восьми лет могут появиться 40–50 тыс. новых стойко-мест», – заключает Д. Горкавенко. **IKS**



**Специальные условия
при оформлении подписки
для корпоративных
клиентов!**



**Оформляйте подписку
в редакции – по телефону: +7 (495) 150-6424
или по e-mail: podpiska@iksmedia.ru**



«Большая тройка» и «большая стройка»

О формировании «большой тройки» на рынке коммерческих ЦОДов, дефиците стойко-мест, эффективности мер господдержки и планах развития сети дата-центров DataPro – исполнительный директор этой компании Евгений Богданчиков.



– Евгений, еще несколько лет назад вы заметили, что в России формируется «большая тройка» операторов коммерческих ЦОДов. Насколько эта тенденция стала более выраженной? Как меняется ландшафт рынка?

– Можно сказать, что тройка лидеров на данный момент сформировалась. (По данным iKS-Consulting, в топ-3 входят компании «Ростелеком-ЦОД», DataPro и IXcellerate. – *Прим. ред.*) И все ее представители реализуют масштабные планы развития. «Ростелеком-ЦОД» активно создает сеть ЦОДов как в Москве, так и в регионах. У нас и у IXcellerate большие инвестиционные программы в Москве. Поскольку идет постоянное строительство, сложно сказать, у кого сколько будет стоек к концу этого года. Но мы понимаем, что к концу 2022 г. при успешном осуществлении планов у DataPro и IXcellerate будет примерно по 8–10 тыс. стоек. Тем самым «большая тройка» еще больше оторвется от других игроков рынка.

Но продолжение M&A-активности, которую мы наблюдали в последнее время, может привести к радикальной смене ландшафта рынка. Я имею в виду покупку «Росэнергоатомом» питерского дата-центра Xelent, а «ЭР-Телекомом» совместно с партнерами – российских активов компании Linxdatacenter. Если эти две компании продолжат активные действия на рынке ЦОДов – «Росэнергоатом» анонсировал строительство дата-центра на 2 тыс. стоек в Иннополисе (Татарстан), может купить также один из крупных строящихся ЦОДов в Москве, а «ЭР-Телеком» планирует строительство объектов в Москве и Перми и т.д., – то состав «большой тройки» может измениться или она превратится в «большую пятерку».

Не исключаю других крупных слияний и поглощений, что может круто поменять расстановку сил на рынке.

– Наличие нескольких крупных игроков, существенно опережающих других участников рынка, – это мировая практика?

– Консолидация на любом развитом рынке – абсолютно нормальный процесс. Большие тройка, четверка или пятерка присутствуют во многих индустриях во многих странах.

Такая ситуация наблюдается и на рынке коммерческих ЦОДов, специализирующихся на услугах colocation. Причем многие, в первую очередь американские, провайдеры являются лидерами не только на рынке своей страны, но и на глобальном рынке. Недавно мы стали свидетелями волны приобретений на европейском рынке (когда американские провайдеры покупали локальных), вызванной ужесточением европейских законов о локализации данных. Сегодня в странах Европы многие ведущие коммерческие ЦОДы либо прямо, либо косвенно принадлежат американским корпорациям.

– Каковы планы развития DataPro как одного из крупнейших локальных игроков?

– Сегодня DataPro управляет двумя дата-центрами совокупной емкостью около 3600 стоек и обслуживает более 150 клиентов. Дальнейшее развитие компании будет происходить на новой площадке на западе Москвы (ул. Рябиновая, 53), где будут построены еще четыре дата-центра.

Наша краткосрочная стратегия предполагает запуск до конца текущего года двух новых дата-центров – DataPro III и IV – суммарной емкостью около 5 тыс. стоек с выходом на полную мощность к концу 2022 г. Также мы планируем в ближайшее время получить всю необходимую разрешительную документацию на строительство второй очереди ЦОДа DataPro I, что позволит расширить его еще примерно на

1,5 тыс. стоек. Решение о начале строительства будет принято в I квартале 2022 г.

Таким образом, реализация краткосрочной стратегии приведет к формированию портфеля из четырех дата-центров совокупной емкостью 8–10 тыс. стоек. С операционной и финансовой точек зрения это достаточный размер для выхода компании на IPO. Если такое решение будет принято, то мы рассмотрим целесообразность слияния с кем-либо из действующих игроков для увеличения доли рынка и соответственно инвестиционной привлекательности компании.

Следующим этапом развития станет строительство нового ЦОДа DataPro V. Предполагается строительство с нуля нового здания площадью около 35 тыс. кв. м и емкостью ориентировочно 7 тыс. стоек. Первую очередь мы планируем запустить в конце 2023-го – начале 2024 г.

По заполнении клиентами DataPro V будут начаты работы над следующим ЦОДом. DataPro VI будет располагаться в существующем здании площадью 60 тыс. кв. м и вместит около 8 тыс. стоек.

Получается, что на новой площадке будут размещаться четыре ЦОДа суммарной емкостью 20 тыс. стоек, общая мощность площадки – порядка 200 МВт. В совокупности с уже имеющимися объектами это составит более 25 тыс. стоек.

– Московский рынок находится в состоянии дефицита стойко-мест. Надолго?

– Давайте считать. DataPro в настоящий момент строит площадки в общей сложности на 5 тыс. стойко-мест. Из них более половины, 3 тыс. стойко-мест, законтрактовано, и мы рассчитываем законтрактовать большую часть оставшегося объема до конца текущего года. Получается, свободных стойко-мест почти не останется. Насколько я знаю, в других коммерческих ЦОДах ситуация схожая.

При этом во многих отраслях мы видим существенный разрыв в степени цифровизации между лидером (или несколькими лидерами) и другими крупными игроками. Например, в банковской сфере такой явный лидер – это Сбербанк, в ритейле – X5 Retail Group и «Магнит» и т.д. Другие игроки будут стремиться для удержания своих рыночных позиций догонять лидера, наращивая ИТ-ресурсы. Это позволяет предположить, что большой объем заказов у нас сохранится еще минимум года два-три.

– А почему заказчикам не уйти в облака?

– DataPro фокусируется на работе с крупными заказчиками – ведущими компаниями в своих отраслях, и мы видим, что большинство из них рассматривает облако в первую очередь как прекрасный инструмент, позволяющий в короткие сроки получить значительный объем ИТ-ресурсов или сервисов для решения срочных задач. Однако все «боевые системы» компании предпочитают держать на своем «железе», а это экономически выгоднее делать в коммерческом ЦОДе.

При этом мы, безусловно, видим быстрый рост бизнеса облачных провайдеров, что заставляет их расширять свои платформы и, как следствие, увеличивать запросы на colocation. А поскольку многие из них – наши клиенты, мы становимся бенефициаром их развития.

– В 2021 г. все дорожает: металл, стройматериалы... Как это скажется на стоимости строительства ЦОДов? стоимости стойко-места?

– Да, цены выросли. Существенно подорожала и рабочая сила. Но в общих капитальных затратах на ЦОД «стройка» не самая большая статья расходов. Самая большая – это оборудование. А у нас – полагаю, что и у других крупных игроков, – с ведущими вендорами заключены долгосрочные контракты, в которых цены зафиксированы. Так что больших проблем я не вижу.

– Как вы прокомментируете подписанный премьером Михаилом Мишустиним второй пакет мер поддержки ИТ-отрасли, в котором фактически предлагается запретить госорганизациям строить дата-центры на бюджетные средства?

– Об отказе от госЦОДов мы говорили давно. Это самая простая и разумная мера поддержки, причем мера, выгодная для всех. Государство не тратит огромные деньги на дорогие стройки, а коммерческие ЦОДы получают новых клиентов и толчок к дальнейшему развитию. Но будет непросто найти в ЦОДах площади для размещения «государственных стоек». Хотя, скорее всего, большая их часть уйдет в «Ростелеком-ЦОД». Но в любом случае я всячески поддерживаю это решение.

– В условиях, когда стойко-места резервируются еще на этапе строительства, казалось, может возникнуть соблазн сэкономить, предложив менее надежные сервисы. DataPro, наоборот, пошла по пути повышения надежности своих ЦОДов.

– Мы стремимся построить лучшую компанию на рынке дата-центров России, и сертификация Uptime Institute – лучшая гарантия надежности и качества наших объектов. Поэтому мы планируем поэтапно сертифицировать все наши дата-центры.

ЦОД DataPro I сертифицирован на соответствие Tier III, а в сентябре прошел повторную сертификацию на Operational Sustainability уровня Gold. До конца года завершится сертификация DataPro II на Tier IV в категории Design. В дальнейшем он будет сертифицирован на Tier IV Facility. Все наши новые дата-центры также будут сертифицированы на соответствие Tier IV.

Существует мнение, что запросов клиентов на Tier IV практически нет. Что ж, считайте, что предоставление сервисов Tier IV – это наша добрая воля. DataPro хочет предлагать максимально высокую надежность, самый лучший сервис. И в целом мы стремимся к тому, чтобы стать первой в России, а возможно, и в Европе, сетью сертифицированных дата-центров Tier IV.

Беседовал Александр Барсков

Новая эра: ЭДО в медицинских организациях

Владимир Соловьев, эксперт, «Нетрика Медицина», генеральный директор, «ЭлНетМед»

Регуляторы подталкивают медорганизации к ведению документации в электронном виде. Это приведет к росту спроса на услуги хранения и обработки медицинских данных, что станет еще одним стимулом развития рынка ЦОДов и облачных сервисов.

В течение последнего года участники системы здравоохранения получили сразу два правовых акта, которые приближают эру безбумажного документооборота в медицинских организациях. Первый – Приказ Минздрава России от 07.09.2020 № 947н, вступивший в силу с 1 февраля 2021 г., – касается порядка ведения медицинской документации в форме электронных документов. Этот документ участники системы здравоохранения ждали давно, поскольку именно он позволяет вести медицинскую документацию исключительно в электронном виде, без дублирования на бумажном носителе. В настоящее время приказ носит рекомендательный характер и определяет требования к формированию, подписанию, хранению и визуализации электронных документов медицинского учреждения. Второй акт, изданный 1 июня 2021 г., уже носит обязательный характер – это Постановление Правительства РФ № 852 о лицензировании медицинской деятельности, которое предписывает медицинским учреждениям передавать данные об оказанной медицинской помощи на федеральный уровень – в Единую государственную информационную систему в сфере здравоохранения (ЕГИСЗ) – в электронном виде.

Иными словами, в настоящее время действуют два взаимодополняющих правовых акта: один разрешает вести документацию медучреждения в электронном виде, другой обязывает именно в таком виде передавать сведения из медицинской организации на федеральный уровень. Стоит отметить, что перечень сведений, которые медорганизация должна переда-

вать на федеральный уровень, постоянно расширяется: сегодня в него входят около 80 документов, но ожидается, что уже к концу текущего года к ним добавятся еще 30.

По сути, эти правовые акты открывают для медицинских организаций новую эру электронного документооборота (ЭДО), который даст возможность клиникам оперативно обмениваться данными не только между собой, государством, но и с пациентами. А это значит, что в не столь отдаленной перспективе можно будет забыть про архивы бумажных карт, бумажные выписки из историй болезни, которые пациент должен был носить с собой при консультации у разных специалистов в разных клиниках, и т.п.

Как клинике перейти на ЭДО?

Чтобы начать вести ЭДО, клиника первым делом должна подключиться к ЕГИСЗ. Сегодня существуют три способа: прямое подключение медицинской информационной системы клиники (МИС) к ЕГИСЗ, подключение МИС клиники к региональной системе (ГИСЗ), которая взаимодействует с ЕГИСЗ, и наконец, способ, оптимальный для большинства частных клиник с точки зрения удобства, оперативности и минимизации финансовых и трудовых затрат – подключение к ЕГИСЗ через оператора иной информационной системы. Способ подключения к ЕГИСЗ клиника выбирает самостоятельно.

Следующий этап – издание в клинике локального акта (приказа) о том, что она будет вести медицинскую документацию в электронном виде. Если речь идет о коммерческих клиниках,

оказывающих пациентам платные услуги, то в договор об оказании медицинских услуг необходимо добавить пункт, информирующий пациента о ведении медицинской документации в электронном виде и предоставлении сведений об оказанной помощи в ЕГИСЗ, а также включить этот пункт в согласие на обработку персональных данных пациента.

Электронные медицинские записи имеют ту же юридическую силу, что и бумажные документы, заверенные подписью и печатью. При этом электронные документы всегда доступны для пациента и его лечащего врача.

Итого, в два несложных шага значительный объем бумажной документации клиники может быть переведен в электронный вид. Однако и тут есть нюансы.



Медицинскую документацию в зависимости от ее характера положено хранить от одного года до 50 лет, а связанную с медико-социальной экспертизой – 75 лет. Вся документация, за редким исключением, содержится в выдавшей ее организации. Причем не важно, государственное это учреждение или частная клиника, правила оформления и хранения документов одинаковы, а за их несоблюдение предусмотрена административная ответственность. Как только клиника переходит на ЭДО и издает первый электронный документ, который выдается пациенту, она должна хранить его не менее 25 лет. С одной стороны, с этим нет особых проблем – современные технологии позволяют хранить данные и более длительный период. Однако если хранение электронного медицинского архива ложится на плечи медицинской организации и ее ИТ-специалистов, то нужно учитывать, что процесс этот будет весьма затратным с точки зрения и финансовых, и технологических, и людских ресурсов. Стоит также отметить, что в настоящее время нормативных актов, регулирующих порядок архивирования медицинских документов в электронном виде, не существует. Эти регламенты пока находятся в стадии формирования и должны будут появиться в течение ближайшего года или двух.

Еще один момент – срок годности электронного медицинского документа, подписанного ЭЦП врача. Сегодня срок действия ЭЦП составляет один год. Чтобы обеспечить юридическую значимость электронной медицинской документации в последующем периоде на федеральном уровне (в ЕГИСЗ), реализована подсистема Регистра электронных медицинских документов (РЭМД). Подписанный ЭЦП врача электронный документ регистрируется в РЭМД, что подтверждает его неизменность и легитимность при хранении в системе на протяжении 25 лет и более. Таким образом решается вопрос юридической значимости электронных медицинских документов.

Как массовый переход клиник на ЭДО скажется на ИТ-рынке?

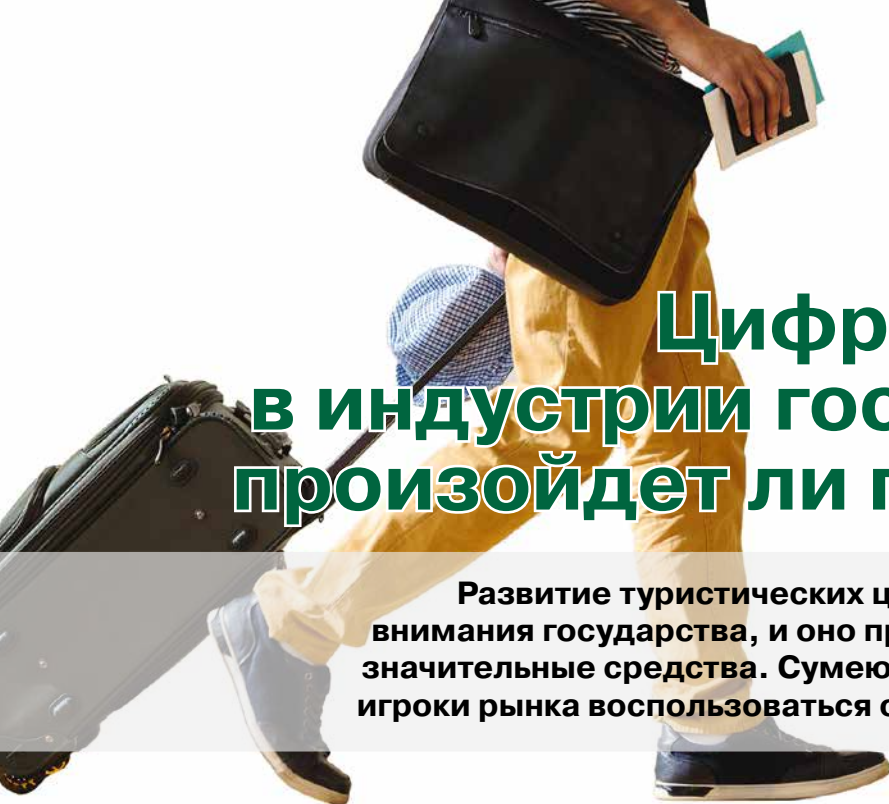
Во-первых, можно смело прогнозировать, что развитие и повсеместное внедрение ЭДО в медицинских учреждениях в ближайшей временной перспективе приведет к количественному и качественному росту спроса на услуги дата-центров. Уже сегодня размещать свои ресурсы в надежных ЦОДах взамен создания собственных серверных считается хорошим тоном.

Во-вторых, однозначно вырастет спрос на размещаемые в ЦОДах дисковые массивы, в которых организуется архивное хранение. В настоящее время на рынке функционируют примерно 60 тыс. клиник частных форм собственности и около 15 тыс. государственных медорганизаций. Учитывая, что около 50% медпомощи оказывается частными клиниками, несложно подсчитать потенциальный объем электронных документов, генерируемых в сегменте частной медицины. Если отталкиваться от объемов данных, хранящихся в ЦОДах, которые работают с информацией ЕГИСЗ и в которых объем дисковых хранилищ сегодня исчисляется петабайтами, то становится понятно, что частная медицина может сгенерировать данных в три-четыре раза больше.

В-третьих, появится спрос и на обработку медицинских данных. Формировать обезличенные статистические массивы, подключать системы искусственного интеллекта и машинного обучения захотят многие игроки этого рынка.

В-четвертых, появятся новые сервисы для пациентов. Например, предоставление доступа к медкарте пациента для клинических исследований, удаленных консультаций с нужными специалистами, оптимизации процессов здоровьесбережения, скоринга для банков и страховых компаний за дополнительную скидку и прочее.

Налицо тренды к упрочению позиций и укрупнению рынка ИТ-услуг в здравоохранении. **ИКС**



Цифровые сервисы в индустрии гостеприимства: произойдет ли перезагрузка?

Развитие туристических цифровых сервисов попало в сферу внимания государства, и оно предполагает направить на эти цели значительные средства. Сумеют ли региональные власти и другие игроки рынка воспользоваться открывающимися возможностями?

Татьяна Толмачева,
управляющий
партнер,
Светлана Патрикеева,
аналитик,
iKS-
Consulting

Когда настает время отпуска, мы покидаем стены своего дома, чтобы отдохнуть от работы, окружения, повседневных обязанностей. Мы покупаем готовый турпакет или планируем собственный маршрут, а с ним – достопримечательности, сервис, комфорт, впечатления и эмоции. И хотя 2020 г. был худшим в истории туристической отрасли, отдыхающие уже подстроились под новую постковидную реальность, переориентировавшись на внутренний туризм. Кризис заставил туристическую отрасль искать новые возможности для выживания, коронавирус ускорил цифровизацию отрасли, изменяя наши привычки и традиционное потребительское поведение.

По данным исследования, проведенного сервисом Tutu.ru в 2021 г., четверть отпускного бюджета у российских путешественников уходит на оплату билетов или бензин и аренду машины, почти четверть суммы они тратят на питание, 22% – на проживание, 20% – на досуг.

Новые цифровые привычки путешественников

При организации поездки туристу нужно решить множество вопросов, от которых зависит, насколько успешно пройдет отпуск: какой тип отдыха выбрать? куда отправиться? как туда добраться? где жить? что посмотреть? чем пи-

таться? Ответы на эти вопросы турист подбирает в зависимости от бюджета поездки, сезона, собственных предпочтений, пожеланий спутников, рекомендаций знакомых, предыдущего опыта, советов туристических ресурсов и т.д.

Исследования говорят о том, что сегодня две трети путешественников полностью или частично планируют поездки самостоятельно с помощью онлайн-сервисов и приложений.

Мы уже привыкли к целому ряду цифровых сервисов, которые упрощают нам выбор, экономят ресурсы, как денежные, так и временные. Например, виртуальный путеводитель помогает грамотно составить маршрут, а в некоторых случаях может стать карманным гидом. Сейчас подобным функционалом обладают как коммерческие приложения, так и региональные порталы. Приложения-переводчики позволяют преодолеть языковой барьер. Сервисы виртуальных экскурсий дают возможность заранее ознакомиться с маршрутом или местом будущего проживания. Для тех, кто отправляется в поход и кому важно иметь доступ к картам местности в любой точке маршрута, существуют специализированные интерактивные сервисы.

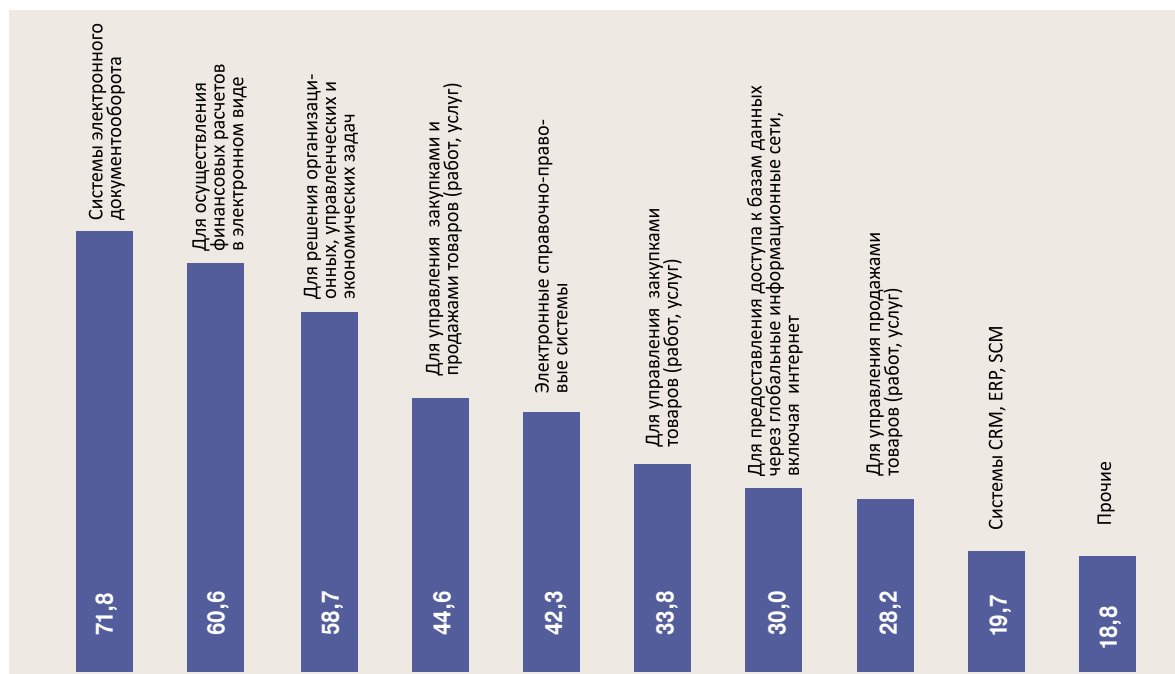
Поиск билетов, туров, отелей, кафе/ресторанов облегчают различные маркетплейсы и агрегаторы. Действуют также специальные площадки для поиска гидов, спутников, фотографов и т.п. Сэкономить можно, например, благодаря использованию карты гостя, которые постепенно вводятся в ряде российских регионов.

Оформить страховку путешественники могут, не выходя из дома, через банковские приложения. Улучшают клиентский опыт и разнообразные способы оплаты, включая бесконтактные технологии, и интерактивные путеше-

Словарь ИКС

➔ В последнее время получил распространение термин «**индустрия гостеприимства**», который охватывает целый ряд подотраслей различных секторов экономики, включая всю туротрасль, а также смежные сферы – общественное питание, транспорт, развлечения и досуг, физкультуру и спорт.

➔ **Туристом** мы называем того, кто хотя бы на один день выезжает из своей территориальной налоговой юрисдикции и покрывает в этой поездке расходы на потребности во время путешествия.



◀ Использование программных средств турагентствами и прочими организациями, предоставляющими услуги в сфере туризма (%)

Источник: iKS-Consulting по данным Росстата, 2019, множественный выбор

ствия. В скором времени появится возможность привлечь к планированию путешествий искусственный интеллект, анализирующий предыдущие запросы и на их основе предлагающий наиболее привлекательные варианты.

В ходе исследования «Цифровые сервисы операторов связи», проведенного iKS-Consulting в начале 2021 г.*, мы насчитали более 125 цифровых сервисов для путешественников. Самыми многочисленными оказались информационные порталы, сервисы онлайн-бронирования и метапоисковики. В рассмотренных сервисах их доля составила 48, 29 и 13% соответственно. Оставшиеся 10% – это отдельные сервисы построения маршрутов и виртуальных путешествий.

По состоянию на середину 2021 г. в общей структуре онлайн-продаж индустрии гостеприимства не менее 60% приходилось на сервисы онлайн-бронирования. На рынке присутствуют десятки игроков, как крупных международных, так и небольших региональных компаний.

* Подробнее см. Толмачева Т. Трудные дети дойной коровы, или Цифровые сервисы операторов связи. «ИКС» № 2'2021, с. 16.

«Цифры» еще недостаточно

Несмотря на активное использование туристами цифровых сервисов, туристическая отрасль пока менее цифровизирована, чем другие сектора российской экономики, а доля интернет-экономики в сфере туризма (онлайн-сервисов для путешественников) в 2020 г. не превысила 2%.

Такое положение дел обусловлено в первую очередь тем, что около 80% всех туристических предприятий – это компании малого и среднего бизнеса, сильно зависящие от сезонности и постоянно сталкивающиеся с дефицитом средств на долгосрочные проекты развития, к которым относятся проекты внедрения информационных технологий и цифровизации.

Важным драйвером цифровизации отрасли в последние несколько лет стали обязательные регуляторные требования предоставления отчетности в ФНС России, ФСС России, ПФР и иные ведомства. Именно поэтому наиболее популярными программными средствами, используемыми компаниями из сферы туризма, гостиничного бизнеса и общепита, являются СЭД, ПО для осуществления финансовых расчетов в электрон-



◀ Типы цифровых сервисов в сфере туризма

ном виде, а также для решения организационных, управленческих и экономических задач.

Для гостиничного бизнеса и общепита значимы также автоматизированные системы, позволяющие управлять закупками и продажами, электронные справочные правовые системы. Для компаний, оказывающих туристические услуги, подобные сервисы менее важны. Стоит отметить, что только пятая часть компаний отрасли использует CRM (см. рисунок), хотя работа с клиентами – основа туристического бизнеса.

Гостеприимство как государственный приоритет

В 2021 г. туристическая отрасль вошла в сферу инициатив государственной поддержки. В апреле был представлен (но пока не утвержден) национальный проект «Туризм и индустрия гостеприимства», в котором уделяется большое внимание цифровизации туризма и распространению туристских онлайн-сервисов.

Интерес к сфере туризма со стороны государства не случаен. Индустрия гостеприимства решает важные экономические, социальные и даже геополитические задачи. Туротрасль уже стала важным звеном глобального человеческого, информационно-культурного и денежно-финансового обмена, элементом сервисной экономики. Кроме того, туротрасль оказывает мощное мультипликативное влияние на экономику в целом, развивая несколько десятков смежных отраслей.

Составляющие нацпроект федеральные проекты «Развитие туристской инфраструктуры», «Повышение доступности туристских услуг», «Совершенствование управления в сфере туризма» станут мощным драйвером цифровизации индустрии туризма и гостеприимства в России.

На реализацию нацпроекта до 2030 г. из федерального бюджета планируется выделить 529 млрд руб., еще 72 млрд руб. – из региональных бюджетов. Средства предназначаются на создание туристической инфраструктуры и развитие территорий, что позволит обеспечить высокий уровень приема и сопровождения

путешественников. Предусмотрено также привлечение внебюджетных частных инвестиций на создание инфраструктуры.

Поскольку на развитие территорий будут направлены серьезные государственные средства, за внимание туристов начнут бороться не только бренды, но целые города и даже регионы.

Цифровизация туристической отрасли в регионах уже отслеживается в рамках индекса цифровизации городского хозяйства «IQ городов». Субиндекс «Туризм и сервис» характеризуется четырьмя показателями:

- наличие электронных карт гостя города;
- наличие комплексной системы информирования гостей города;
- количество уникальных активных пользователей электронных карт города;
- востребованность системы информирования гостей города (количество просмотров онлайн-портала города на 10 тыс. человек его населения).

Цифровизации туротрасли посвящена подпрограмма совершенствования управления отраслью на основе данных. С помощью информационных технологий планируют получать полные статистические данные о туристах, туристических потоках, популярности тех или иных направлений и спросе в туризме. Обсуждается возможность закупки данных у мобильных операторов. Аналитический центр при Правительстве РФ работает над единой методологией оперативного сбора данных в регионах, что позволит прогнозировать и быстро оценивать загрузку по тем или иным направлениям и принимать соответствующие управленческие решения. Планируется, что все услуги в туризме в течение ближайших трех лет станут цифровыми.

Туризм превращается в действенный инструмент для привлечения инвестиций в регион, совершенствования существующей туристической инфраструктуры, развития туристических кластеров. Поэтому региональные чиновники сейчас уделяют большое внимание маркетингу территорий и продвижению своих регионов в рейтинге локаций для путешествий.



Проекты в сфере цифровизация индустрии гостеприимства

Москва поддерживает развитие цифровых сервисов и приложений для отрасли, например, проводит туристический хакатон Moscow Travel Hack и акселерационную программу для стартапов «Фабрика туристических продуктов и сервисов» под брендом отраслевого сообщества Мостуризма Moscow Travel Hub.

Московская область запустила и развивает порталы welcome.mosreg и VisitMO.

Компания «Русатом инфраструктурные решения» госкорпорации «Росатом» презентовала проект цифровизации Мурманска и создания портала для Мурманской области как технологичного маркетингового решения для туротрасли.

«**Я**ндекс» активно подписывает с регионами соглашения о стратегическом партнерстве в вопросах цифровизации туротрасли.

Уникальный торговый продукт в индустрии гостеприимства сможет стать дополнительным элементом УТП «Умный город».

Утверждение национального проекта для туристической отрасли позволит решить много задач, от которых зависит реализация концепции управления индустрией туризма на основе данных. В числе этих задач:

- создание нормативной основы для обмена данными между участниками рынка и ведомствами;
- отработка бизнес-моделей обмена данными между участниками рынка;
- организация межведомственного взаимодействия, создание технической инфраструктуры для обмена данными.

Формирование туристской экосистемы, объединяющей всех участников рынка на онлайн-платформе и интегрированной с внешними источниками данных и социальными платформами, послужит улучшению клиентского опыта.

Операторы связи для туристической индустрии

Подготовка и запуск национального проекта усилили интерес разных компаний и организаций к индустрии гостеприимства. В 2020–2021 гг. участники этого рынка заметно активизировали свою деятельность в направлении цифровизации туристической отрасли и управления ею на основе данных. Обсуждается вопрос о создании цифрового профиля региона и цифрового профиля туриста – инструментов, которые позволят эффективно управлять индустрией.

Не остались в стороне и операторы связи. Они уже несколько лет развивают экосистемы цифровых сервисов и включают в них услуги в сфере туризма для конечных потребителей, для государства, для компаний отрасли.

Операторы связи сотрудничают с отдельными регионами и кроме виртуальных путеводителей предлагают масштабные решения с использованием геоаналитики и больших данных, которые позволяют анализировать информацию о туристических потоках. Эта информация помогает местным администрациям оптимизировать затраты на инфраструктуру для туристов, корректировать маршруты и расписание общественного транспорта, планировать культурные мероприятия. Например, ДИТ Москвы закупал у операторов связи геоаналитику, чтобы отслеживать перемещения горожан и на основе этих данных вносить изменения в работу городского транспорта и инфраструктуру. По экспертным оценкам, с 2015-го по 2020 г. на закупку геоаналитической информации у сотовых операторов связи из бюджета Москвы было выделено более 700 млн руб.

На рынке туристических цифровых сервисов операторы связи имеют колоссальное преимущество благодаря огромному пулу клиентских данных, анализ которых в обезличенном виде позволяет получать информацию о туристических потоках, наиболее привлекательных туристических объектах, динамике перемещений. Сотрудничество с регионами, отработка механизмов анализа данных и использования результатов позволяют тиражировать сервисы во всех субъектах РФ.

Сервисы B2B в основном представлены предложениями для решения традиционных бизнес-задач (коммуникация, совместная работа, управление взаимоотношениями с клиентами, электронный документооборот и т.п.), решений для туристской инфраструктуры. Многие из этих предложений актуальны и для туроператоров, турагентств, компаний гостиничного и ресторанного бизнеса. Доработка имеющихся предложений с учетом специфики деятельности туристических компаний, а также использование новых технологий (бесконтактные технологии, виртуальная и дополненная реальность, автономные системы обслуживания и др.) позволят привлечь больше заказчиков из туристической отрасли.

Окно возможностей для цифрового туристического будущего

По оценкам iKS-Consulting, в 2020 г. общие расходы на информационные технологии и услуги связи в отрасли туризма и гостиничного хозяйства не превысили 3 млрд руб. Порядка 80% этой суммы – это расходы на услуги связи, приобретение ИКТ-оборудования, а на цифровые сервисы пришлось не более 3% ИКТ-расходов отрасли.

Такие объемы потенциального рынка малопривлекательны для крупных технологических игроков с точки зрения масштабных инвестиций в цифровые сервисы. Очевидно, что только в случае реализации мер государственной поддержки и финансирования мероприятий национального проекта государством небольшие пилоты и точечные проекты цифрового туризма смогут привести к цифровой перезагрузке отрасли. Это вполне возможно, если государство будет быстро осуществлять намеченные планы в области индустрии гостеприимства.

В 2020–2021 гг. благодаря закрытым из-за пандемии границам внутренний туризм избежал конкуренции с международным. Но рано или поздно ситуация изменится, границы для российского туриста откроются. Это означает, что у российских регионов достаточно небольшое «окно возможностей», за которое нужно многое успеть сделать, включая развитие туристических сервисов, чтобы привлечь и удерживать новых путешественников. **ИКС**

Апология инженерии

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

Голос инженеров, такой негромкий, заглушаемый речевками и заклинаниями финансистов, экономистов и маркетологов всех мастей, звучит все слабее. Но престиж (или его отсутствие) инженерного сообщества – показатель индустриализации/деиндустриализации страны.

Я – инженер на сотню рублей,
И больше я не получу...
Борис Гребенщиков

Инженерное сословие уходит из сферы телекоммуникаций и ИТ. Так было уже неоднократно с разными отраслями техники. В начале XX века инженер-электрик вне зависимости от происхождения был в провинции членом дворянского собрания. А уже в середине XX века он превратился в малоуважаемую личность в ЖЭКе, иногда спивающуюся, «а-ля Афоня». Но до того был проект ГОЭЛРО, было строительство Днепро-ГЭСа, создание, а после войны полная реконструкция единой энергосистемы страны. В результате все было отлажено, и инженеры сменились техниками на местах. Однако в энергетике были и остаются еще инженеры «от Бога», отвечающие за турбины электростанций, АЭС и пр.



Упадок и разрушение инженерного мировоззрения

Но как объяснить, что во время реализации проекта «Цифрового ГОЭЛРО» (цифровой экономики), когда технология связи и ИТ на подъеме, а отрасль уже три десятилетия находится в состоянии научно-технической революции, когда вся экономика переводится на новые рельсы и на этой основе строится новый экономический уклад, во время всех этих технических преобразований инженеры практически исчезают из нашей отрасли? Их мнение не учитывается, их голос не звучит...

Еще хуже, что системно уничтожается инженерное мировоззрение. А ведь это важная часть всей социальной системы нашего народа, часть нашего культурного кода, залог стратегического

развития страны. Что такое мировоззрение инженера? Это картина мира в расчетных и измеримых категориях. Инженер советского периода – это человек с логарифмической линейкой в кармане. Потому что необходимость расчетов для любой сферы деятельности не подвергалась сомнению. Более того, инженеры любили рассчитывать, выдвигать гипотезы и проверять их в ходе экспериментов. Параметры в описаниях должны быть измеримы, и измерения эти проверяемы. Картина мира для инженера – это совокупность рассчитываемых и проверяемых/измеримых параметров. А цель деятельности – поиск правил расчета и проверки/эксперимента.

В начале XX века инженера нельзя было рассматривать как человека, обслуживающего механизмы. Мир перестал быть механистичным уже в эпоху пара. Знание термодинамики и электродинамики стало необходимым. Но от прошлого механического мира осталась вера в строгость правил и однозначность проверки. Логарифмические линейки сменились более удобными калькуляторами: сначала программируемыми, потом портативными. Им на смену пришли компьютеры, с помощью которых сейчас можно решать любые инженерные задачи. Но бума инженерной мысли не возникло. Престиж инженера падает, а мировоззрение разрушается.

Современные научно-технические конференции вполне можно назвать финансово-маркетинговыми. Богатые спонсоры в режиме сугубо вещательной презентации рассказывают об эффективности, окупаемости, монетизации и новых веяниях на Западе и Востоке. В их докладах нет показателей, да этого уже и не ждет аудитория, ей количественные и измеримые категории скучны и непонятны. Квинтэссенцией такого шоу можно считать демонстрацию, на которой серьезный с виду докладчик аргументировал свою правоту фразой: «Как видите, компьютер показал...». Знание распадается: расчетные модели отдельно, эксперименты отдельно, развитие и внедрение технологий отдельно. Эти части единого некогда целого теперь оказываются несвязанными, разделенными и обесцененными.

Модели не проверяются экспериментально. Результаты моделирования никак не влияют на настройку сетей. Внедрение в практику притаилось где-то в глубине диссертаций, которые перестали быть носителями новых научных подходов. Сердце инженерии бьется нечетко, пульс нитевидный...

От инженерии к магии

На смену инженерному мировоззрению приходит более древнее, мифологическое и магическое. Известная шутка гласит, что, если плохо изучать физику в школе, мир будет наполнен чудесами и магией. Наши научно-технические конференции сегодня заполнены как раз ими в сочетании с призывами маркетингового толка и рассказами о заморских странах, приправленных многозначным местоимением «мы». Когда русский парень, представитель американской компании, рассказывая о проекте в Испании, говорит: «В результате мы получили большой экономический эффект», он торгует самым сладким маркетинговым наркотиком – сопричастностью. Американцы сделали что-то в Испании и что-то получили. Проверить это нельзя, понять что-либо тоже сложно: в разных странах разные правила игры, разные правила коррупции (извините, лоббирования проектов), разные менталитет и ожидания, разные стратегии развития общества, в конце концов. Но многозначное «мы» позволяет соединить и нас, в России, с великими достижениями мировой технологии. Тем более что это «мы» говорит симпатичный соотечественник с поставленной речью. Инженерная составляющая подобных докладов ниже нуля, поскольку они отравляют, оболванивают и убаюкивают аудиторию одновременно, а таких докладов – большинство.

Капитализм, рынок и конкуренция добавляют разобщенности. Попробуйте с трибуны заявить о своей инженерной ошибке, пусть и под соусом: «Коллеги, не попадайтесь на удочку, не работает эта штука!». Сразу скажут: «Эта компания/коллектив/группа явно непрофессионалы», раскритикуют, опровергнут. Да и пиарщики такие доклады не пропустят, ведь подобные слова бросают тень на серьезную нашу компанию. Потому что серьезные компании не ошибаются. Коммерсанты произнесут свое заклинание: «Не высывайтесь. Деньги любят тишину...». Результат налицо – вот уже несколько лет на конференциях, в статьях нет никаких критических инженерных докладов и статей. У каждого инженера, как и у врача, должно быть свое кладбище – инженерные ошибки, неверные расчеты, отброшенные гипотезы. Но это поймет только инженер, коммерсант и маркетолог не поймут.

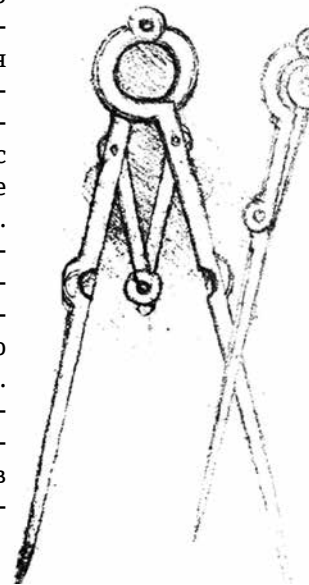
Остались блог-посты на хабре от энтузиастов, отдельные робкие голоса последних инженеров. Энтузиасты разделены – нет мест встречи, где можно поговорить. Такие площадки перестали существовать и на форумах, и на конференциях, и в вузах. Это в советское время любая конференция, семинар превращались в дискуссию, и нужно было использовать инженерную аргументацию.

С измеримостью показателей систем связи еще хуже. Не прошло и 30 лет развития пакетных сетей связи, как понятия «пакет», «пропускная способность канала», «задержка пакета» были легализованы постановлением правительства № 1847 в ноябре 2020 г. Это первые робкие шаги по пути наведения порядка в системах связи. До этого метрология пакетных сетей отсутствовала, отрасли с «регулирующей рукой рынка» она не требовалась. Святой для каждого инженера тезис Д.И. Менделеева «Наука начинается там, где начинаются измерения» был просто забыт. Образовавшийся вакуум заполнили суррогаты, которые на метрологических конференциях называли «фуфлометрами» и «попингуями». Но инженеров нового поколения это вполне устраивало и устраивает до сих пор. Картина мира нового поколения уже не в измеримых категориях, а в догматических рекомендациях зарубежных коллег. Из инженеров они превращаются в техников по обслуживанию заморских технологий.



Инженер формируется тогда, когда решает инженерные задачи. Сам или в группе профессионалов. Только так он может расти. Если инженерных задач нет, инженерное сословие вырождается. В свое время отсутствие в нашей стране масштабных проектов привело к исчезновению главных конструкторов. Отсутствие проектов приводит к вымиранию института просто конструкторов. Следующим плацдармом нашего отступления в сторону банановой республики будет инженерия. Отсутствие инженерных задач может привести к девальвации инженеров как профессионального сообщества. Это и будет завершающим аккордом деиндустриализации нашей страны.

Можно уповать на то, что инженеры самоорганизуются и объединятся, восстановят принципы информационного и профессионального обмена, этический и профессиональный кодексы русской инженерной школы. Можно надеяться, что где-то в недрах останется «старая гвардия инженерии», которая помнит еще славные традиции и сможет передать опыт молодым. Но пока такого движения не видно... И это страшно. ИКС



ЦОД от концепции до модернизации

Александр Барсков

Российская индустрия ЦОДов взрослеет. И признанные лидеры этого рынка стремятся не просто продвинуть свои продукты и услуги, а поделиться накопленным за годы работы опытом. Это особенно ценно для новых игроков, которых рынок дата-центров привлекает своим быстрым ростом.

Взросление отрасли отразилось и в характере контента ее основного форума, организованной «ИКС-Медиа» конференции «ЦОД», прошедшей в этом году уже в 16-й раз. Если в предшествующие годы большую часть выступлений составляли продуктовые доклады вендоров, то в нынешнем году фокус сместился на обсуждение актуальных проблем отрасли и обмен опытом и наилучшими практиками для всех этапов жизненного цикла дата-центра – от идеи и концепции до эксплуатации и модернизации. Это стало наиболее ценной составляющей форума.

Начинаем с идеи и концепции

ЦОД, как и положено любому серьезному проекту, начинается с идеи. Ее слагаемые, как считает Евгений Колосков, технический директор компании «Свободные Технологии Инжиниринг», – это целевые показатели: количество ИТ-стоек, средняя мощность одной стойки, резерв мощности, требования к доступности и отказоустойчивости (например, соответствие уровню Tier II, III, IV или что-либо иное), а также бюджет проекта. Кроме того, желательно уже на этом этапе определить целевые уровни энергоэффективности (PUE) и экологичности (LEED, BREAM) будущего объекта, его внешний облик и учесть особые требования со стороны информационных систем.

Переходя к этапу концепции, выбирают площадку и привязывают идею к ее особенностям. Затем вырабатывают архитектурно-планировочные решения, принципиальные схемы инженерных систем, проводят укрупненную оценку бюджета проекта, эксплуатационных затрат, формируют финансовую модель, график реализации проекта и как итог – техническое задание.

При разработке концепции важно учесть все ограничения площадки. «Площадка может выглядеть привлекательно – чистое поле с минимумом ограничений, но все равно надо провести максимально полный аудит», – рекомендует Е. Колосков. Необходимо учесть вид разрешенного использования (ВРИ может не включать строительство ЦОДа, а на его изменение требуется время); доступность нужных ЦОДу ресурсов (электричества, воды и т.д.); наличие неудобных соседей (опасных производств, жилых объектов и т.п.). Даже если на момент выбора площадки таковые отсутствуют, лучше проверить, не планируется ли их строительство в будущем.

Обязательно нужно проанализировать геоподоснову. «Важно выяснить, что находится в земле, какие сети проложены на данной территории. Нередко переносить такие сети сложно или дорого, – делится опытом эксперт компании «Свободные Технологии Инжиниринг». – Могут

также возникнуть ограничения, связанные с объектами культурного наследия, социально-защитными и экологическими нормами».

Именно на этапе концепции следует рассмотреть все возможные варианты и пожелания заказчика в плане выбора технологий и построения инженерных систем. «Если заказчик хочет попробовать ту или иную технологию, то изучить ее применимость надо именно на данном этапе, – советует Е. Колосков. – Пройдя этап концепции, возвращаться к пересмотру каких-либо решений весьма накладно. “Убегут” сроки реализации, или вы потеряете деньги».

«Лучше избегать уникальных решений – имеются в виду не различные уникальные схемы (они могут быть эффективными), а применение в этих схемных решениях компонентов, которые невозможно заменить другими, – продолжает он. – Уникальные решения от одного производителя могут завести проект в узкое горлышко: если впоследствии этот производитель, например, перестанет поставлять продукты на рынок, вы будете вынуждены пересматривать концепцию».

Неприятие безальтернативности – похоже, главный принцип компании «Свободные Технологии Инжиниринг». Ее генеральный директор Евгений Вирцер считает, что этим принципом надо руководствоваться на всех этапах создания ЦОДа, причем в отношении выбора как поставщиков, так и подрядчиков. «Мы как-то попали в ситуацию, когда в проекте был безальтернативный исполнитель. В один прекрасный момент у него начались серьезные проблемы из-за других объектов, а мы остались связанными по рукам и ногам. Никакой замены подобрать не могли. Сроки строительства сдвинулись на два месяца. Если бы могли заменить поставщика или подрядчика, задержка была бы всего на неделю», – рассказывает он.

Проектируем и строим с помощью BIM

Этап концептуального проектирования Е. Колосков сравнивает с движением по извилистой дороге со множеством развилок, на которой ищешь правильный путь, то сворачивая, то возвращаясь обратно. А вот последующая разработка проектной документации – это, по его мнению, прямолинейное движение с выверенной скоростью, поскольку процедуры на этом этапе сильно формализованы. Регламентированы и процедуры ее сдачи в органы экспертизы. Если проектировщики хорошо знают нормы и правила, то данный этап можно пройти достаточно быстро и безболезненно.

Но и при проектировании есть ряд важных моментов, которым надо уделить внимание.

Один из них – использование систем класса BIM, которые считают обязательными подавляющее большинство экспертов.

«ЦОДы – огромные объекты, но на практике места всегда не хватает. Когда мы использовали 2D-проектирование с типовыми строительными допусками, постоянно возникали нестыковки. Поняли, что надо с 2D переходить на проектирование в 3D. Сейчас модели оборудования закладываем в BIM и вписываем их в здание с точностью до миллиметра, – рассказывает Алексей Солдатов, генеральный директор компании DataPro. – Без BIM-проектирования сегодня сложно построить что-либо высокоплотное и насыщенное инженерными системами, когда требуются минимальные допуски».

Следует также учесть, что трехмерные изображения хорошо понимают даже строители не самой высокой квалификации. А вот в 2D-чертежах порой сложно разобраться, их надо уметь читать.

Само проектирование в BIM может оказаться дороже (по оценке А. Солдатова, примерно в полтора раза), но поскольку стоимость проектирования составляет около 1–2% стоимости ЦОДа, точность и удобство работы с лихвой компенсируют эти дополнительные расходы. А в целом, как утверждает Е. Вирцер, проектирование в BIM обходится даже дешевле – с учетом расходов на переделки, которые постоянно воз-

никают в 2D-проектах. На счету компании «Свободные Технологии Инжиниринг» уже десятки проектов, сделанных с использованием BIM. DataPro четыре своих ЦОДа также проектировала с помощью этой технологии.

Следующий этап – подготовка рабочей документации. На этом этапе проектные документы детализируются до уровня рабочих чертежей, которые используются при строительстве. Рабочую документацию также целесообразно готовить в системе BIM.

Как правило, описываемые этапы накладываются друг на друга. «Надо быть готовым к тому, что стройка начнется еще во время подготовки проектной документации, – говорит Е. Колосков. – В идеале проектный офис должен находиться на объекте, постоянно взаимодействовать с генподрядчиком, заказчиком и строителями. Если рабочая документация выполнена правильно, генподрядчик выбран профессиональный, то задача построить объект в срок, с должным качеством и уложиться в бюджет вполне решаема».

При выборе наилучшей практики для использования в ходе строительства опять встают вопросы, связанные с BIM. «Зачастую BIM “умирает” на этапе проектирования – дальше строители работают с бумагой или электронными документами в формате pdf, – рассказывает Е. Колосков. – Но есть много инструментов, ко-

Курс на комплексные решения

На форуме «ЦОД» ведущие производители продукции для инженерной инфраструктуры ЦОДов по традиции представляют свои новинки. Один из трендов текущего года – растущее число вендоров, которые стремятся предлагать максимально полные решения в этой области.

Vertiv, выпускающая ИБП и блоки розеток (PDU) для систем электроснабжения дата-центров, начала производить элементы, которые располагаются между ИБП и PDU, в частности шкафы и шинопроводы распределения питания в машзалах.

Шкаф Liebert RXA, построенный на базе решения SMISLINE партнера Vertiv компании ABB, дает возможность отключать и подключать устройства и компо-

ненты под напряжением, что увеличивает свободу маневра, когда необходимо менять конфигурацию ЦОДа. Подобный функционал реализован и в шинопроводе Liebert MBX: это решение позволяет устанавливать коробки отбора мощности в любом месте шинопровода без отключения питания в других стойках.

Максим Орехов, технический эксперт Vertiv, анонсировал обновления ИБП средней мощности Liebert EXM2, внутрирядных и шкафных кондиционеров, а также новую линейку чиллеров Vertiv OFC.

Schneider Electric сделала акцент на позиционировании компании как поставщика полного решения

Шкаф распределения питания Liebert RXA компании Vertiv ►



торые позволяют эффективно сопровождать строительство с помощью BIM, создавать облачную среду, в которой можно вносить изменения в документацию, поддерживать ее в актуальном состоянии».

Производители оборудования также активно используют преимущества BIM. Так, компания SME предлагает на базе BIM моделировать выпускаемые ею модульные ЦОДы FlexSize. С помощью этого инструментария заказчик может внести необходимые изменения, например, переставить блоки бесперебойного питания в другое место ЦОДа и т.д. Затем модульный ЦОД изготавливается по получившейся BIM-модели.

Эксплуатируем и модернизируем, учитывая состояние оборудования

«Чем раньше служба эксплуатации включится в работу над проектом, в идеале – с этапа концепции, тем лучше, – считает Е. Колосков. – Участие специалистов по эксплуатации в принятии проектных решений, согласовании изменений помогает не только быстро ввести объект в строй, но и качественно его эксплуатировать».

Цифровизация и использование современных систем мониторинга радикально меняют подходы к эксплуатации инфраструктуры ЦОДов. «Если раньше ремонт проводили, когда что-нибудь ломалось, то сейчас благодаря внедрению систем мониторинга можно делать это по

состоянию оборудования, не доводя до крупных поломок, стоимость устранения которых существенно выше, – рассказывает Юлия Балицкая, директор по операционному маркетингу сервисных услуг компании Schneider Electric. – То же самое с техническим обслуживанием. Можно перейти от регламентного обслуживания к обслуживанию предиктивному. Это позволяет уменьшить объем ТО, сократить расходы». Можно увеличить период между ТО, если системы находятся в хорошем состоянии. Например, заменять АКБ на основе оценки их состояния и расчета остаточного ресурса.

Примером современных цифровых систем, помогающих эксплуатировать ЦОДы, может служить семейство облачных платформ предиктивной аналитики Adviser. Эти системы содержат цифровые модели инженерных систем как самой Schneider Electric, так и других производителей. Собираемые с реальных систем данные анализируются на основе алгоритмов искусственного интеллекта и мнений экспертов, которые подключаются к принятию решений. (Пока общий объем накопленных данных недостаточно велик, поэтому эксперты необходимы.) На выходе – отчеты о состоянии систем, их эффективности, рекомендации о необходимости тех или иных действий и т.д.

«Цифровые инструменты и сервисы позволяют снизить стоимость обслуживания, – утверж-



для системы энергоснабжения ЦОДа – от подстанции до сервера. «Для заказчика важна надежность не отдельных блоков, например ИБП, а системы энергоснабжения в целом, – отметил Алексей Соловьев, технический директор подразделения Secure Power. – Наша компания предлагает все компоненты этой системы, кроме ДГУ».

А. Соловьев отметил коммерческую успешность анонсированного год назад ИБП Galaxy VL (200–500 кВт), а также обновление ИБП Galaxy VS (20–150 кВт) – добавлены технология безопасной «горячей» замены модулей пользователем, возможности программного и аппаратного масштабирования. Причем в Galaxy VL и Galaxy VS используются одинаковые модули, что позво-

ляет иметь один ЗИП и упрощает процедуры обслуживания. Также представитель Schneider Electric анонсировал расширение бюджетной серии Easy выпуском ИБП Easy UPS 3L (250–600 кВт).

Еще одна новинка – серверные блоки розеток NetShelter Switched PDU серии 9000. Их особенности – повышение рабочей температуры эксплуатации до 60°C и уменьшение погрешности измерений до 1%.

SME представила ART Modular – серию решений, объединяющих различные префаб- и модульные конструкции. В эту серию входит, в частности, CrossHub – заменяющий традиционную серверную комнату двухсекционный шкаф с антивандальной защитой, возможностью установки системы кондиционирования и другого оборудования, в том числе модуля пожарной безопасности (разрабо-

◀ NetShelter Switched PDU серии 9000



Рис. 1. Предложенный HTS виртуальный тренажер сервисного обслуживания SmartService ▶

дает Ю. Балицкая. – Так, в новых ЦОДах мощностью от 100 кВА стоимость ТО будет составлять 3–5% стоимости оборудования. Это гораздо меньше, чем несколько лет назад».

Одна из болевых точек процесса эксплуатации ЦОДов – кадровый вопрос. «За 30 лет работы мы реализовали сотни проектов, в том числе на удаленных объектах, – рассказывает Ирина Арепина, заместитель генерального директора компании Hosser Telecom Solutions (HTS). – И постоянно сталкиваемся с тем, что инженеры в удаленных точках не готовы работать со сложным оборудованием. Кондиционеры либо совсем не обслуживают, либо просто протирают тряпочкой». Понятно, что без должного сервисного обслуживания надежность работы оборудования резко снижается, а в случае поломки завод может отказать в гарантийном ремонте.

Чтобы повысить квалификацию сервисных инженеров, HTS предложила виртуальный тренажер SmartService для задач техобслуживания инженерного оборудования ЦОДов (рис. 1). «Пилотов ведь никто не допускает за штурвал, пока они не научатся управлять самолетом на тренажере», – замечает И. Арепина. Система основана на использовании шлема виртуальной реальности и позволяет инженерам отработать все действия как при штатном сервисном обслуживании, так и в нештатных ситуациях. Первый опыт применения этого решения оказался позитивным.

Принцип учета состояния оборудования подходит и для модернизации ЦОДов. Современные системы мониторинга и анализа собираемых данных позволяют спрогнозировать необходимость модернизации в зависимости от состояния систем, а также приоритизировать процедуру модернизации, определив, что нужно менять в первую очередь.

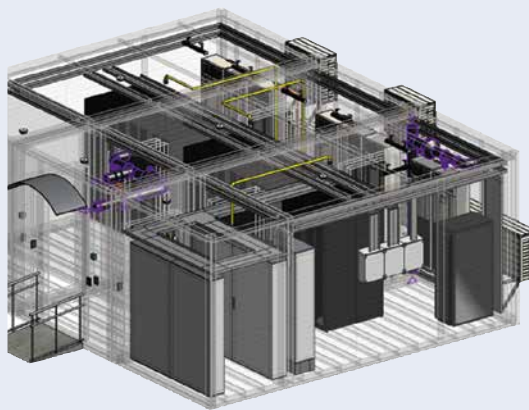
Интересный проект модернизации системы бесперебойного питания представила ГК «Темпесто». В 2019 г. для провайдера «АКАДО Телеком» ее специалисты заменили 15 ИБП (общей мощностью 3 МВт) в работающем ЦОДе без отключения нагрузки. Столь важная операция требовала серьезной подготовки. Как рассказал Леонид Гаврилов, основатель и основной бенефициар ГК «Темпесто», действия были распланированы по секундам, а ДГУ включали максимум на

тан совместно с ГК «Пожтехника»). ART Modular FlexSize – реализуемый на базе силового каркаса модульный ЦОД емкостью от 5 до 200 стойко-мест. Также в серию входят энергомодули (с ИБП и системой генерации – дизельной или газовой), модули физической защиты, оптического кросса и т.д.

Как отметил Александр Никитин, генеральный директор SME Россия, новая линейка решений разработана в России, а ее производство налажено в Московской области. Сотрудничество с компанией Legend позволяет делать ЦОД под ключ, используя ее компонентную базу. Модульные решения SME вне-

дрены в ЦОДе 3data, развернутом на территории индустриального парка «Большое Есипово».

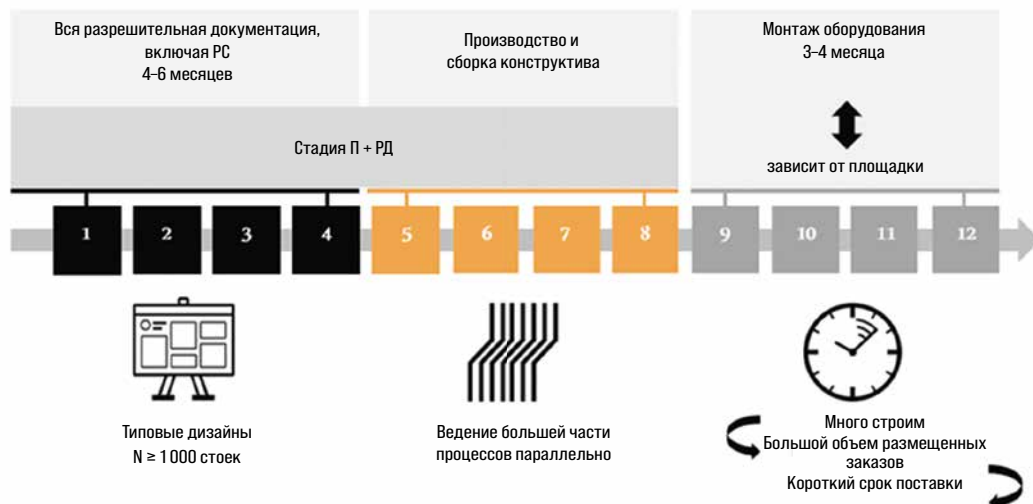
ABB предлагает для крупных ЦОДов модульную систему MegaFlex DPA UPS мощностью до 1,5 МВт. Это производимое в Швейцарии устройство построено на основе запатентованной архитектуры DPA, в которой



◀ **Схема ЦОДа**
на основе решения ART
Modular FlexSize

ИБП среднего
напряжения
компания ABB ▶





◀ **Рис. 2.**
Подход DC development к реализации проектов построения ЦОДов

30 мин при проведении критических переключений. После такой замены (были установлены устройства DPH 500 кВА производства Delta) площадь, занимаемая ИБП, уменьшилась на 60%. Вслед за этим подобные проекты «Темпесто» выполнила еще на двух объектах, а сейчас меняет ИБП в одном из московских ЦОДов.

От стройки века – к стройке года

Несмотря на разработку новых технологических и организационных подходов, позволяющих сократить сроки реализации проектов ЦОДов, пока на ввод в строй объектов емкостью

от 1 тыс. стоек уходит полтора-два года. Новые игроки, выходящие на рынок, полны оптимизма сократить эти сроки до года. Именно такую цель – построить мегаЦОД за один год – преследует компания DC development, входящая в «ПНК Групп». Этот крупный девелопер индустриальной недвижимости ввел в строй уже более 5 млн кв. м различных промышленных объектов.

Опыт и наработки девелопера должны помочь «ПНК Групп» ускорить процессы строительства (рис. 2). «Обычно поиск участка для ЦОДа – один из самых сложных этапов, который занимает шесть месяцев и более, – рассказывает



▲ ИБП Kehua, построенный на базе силовых модулей 125 кВА

каждый модуль – законченный ИБП. КПД устройства в онлайн-режиме достигает рекордного значения 97,4%, а расчетный срок службы – 15 лет. Межсервисный интервал – 7 лет, т.е. за весь проектный срок службы достаточно один раз заменить вентиляторы и силовые конденсаторы.

Для крупных ЦОДов АВВ производит ИБП среднего напряжения – это рассчитанная на напряжение 6, 10, 20, а в скором времени и на 35 кВ модель HiPerGuard MV UPS. Максимальная мощность одного устройства – 2250 кВт, параллельной системы – до 22,5 МВт. Как отметил Евгений Вецпер, менеджер по развитию бизнеса АВВ, выпущенные три года назад, эти ИБП немного опередили свое время, однако по мере укрупнения ЦОДов спрос на них растет. Недавно завод принял заказ на изготовление более 50 таких ИБП общей мощ-

ностью свыше 100 МВт для одного из ЦОДов в США.

Kehua Tech в ответ на пожелания заказчиков увеличить энергетическую плотность оборудования разработала силовой модуль мощностью 125 кВА (высотой 3U). Как сообщил Михаил Богачук, технико-коммерческий директор Kehua Tech, в одном конструктиве (шкафу) ИБП MR33 можно установить до 12 таких модулей, кроме того, восемь шкафов ИБП устанавливаются в параллель – в результате можно получить систему бесперебойного питания на 9,6 МВт.

Конструкция ИБП предусматривает «горячую» замену всех модулей: силовых, модуля управления и модуля электронного байпаса. КПД устройства, которое может комплектоваться как свинцово-кислотными, так и литий-ионными АКБ, в онлайн-режиме составляет около 97%.



▲ Рис. 3. Входная группа ЦОДа DC One

Александр Прибытков, управляющий директор DC development. – У нас ситуация другая: даже если мы не владеем участком, то у нас на примете много других участков, которые можно оперативно приобрести». На получение всей разрешительной документации уходит от четырех до шести месяцев. Как только она получена, «ПНК Групп» начинает изготовление на своих заводах (их у нее пять) конструктивных элементов для здания. Сборка конструктива

объекта площадью 10–20 тыс. кв. м занимает 2–2,5 месяца. «Поскольку строим много, мы постоянно размещаем заказы на большой объем инженерного оборудования. Поэтому, когда приступаем к монтажу оборудования, оно уже все консолидировано на складе. Сейчас это особенно важно, поскольку некоторые заказы, например, на ДГУ, могут доставляться до девяти месяцев», – поясняет А. Прибытков.

Первым объектом, на котором DC development обкатывает свой подход, станет ЦОД DC One в Медведково. Это семиэтажное здание вместимостью до 4 тыс. коммерческих стоек и общей площадью более 24 тыс. кв. м. Проектная мощность – 36 МВт. Решения применяются классические (чиллерная система охлаждения), но эффективные, что должно помочь обеспечить PUE на уровне 1,2. В состав комплекса входят как технологическая зона, так и офисная часть. DC development серьезно подходит не только к технологии создания ЦОДа, но и к презентабельности своих объектов. Как сообщил А. Прибытков, над дизайном здания работало европейское бюро (рис. 3).

Второй объект – DC Two – готовое мультифункциональное (логистическое) здание, которое адаптируется для ЦОДа. Его емкость 8,5 тыс. стоек: 4 тыс. стоек – второй этаж, 4,5 тыс. – первый. Развитие планируется в течение трех лет.

В центре внимания – охлаждение

Ряд компаний, имеющих в своем арсенале полный комплекс инженерных решений для дата-центров, на форуме «ЦОД» сделали акцент на оборудовании охлаждения.

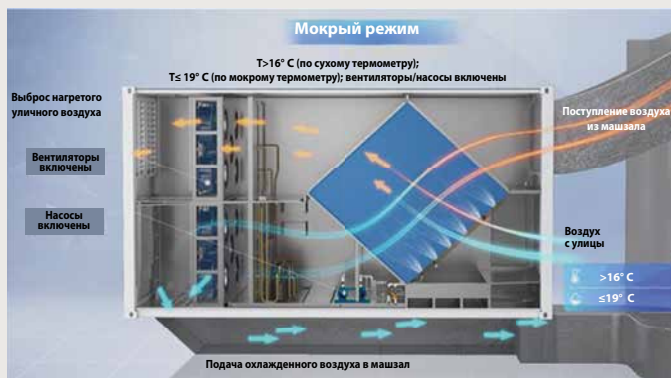
Huawei представила систему FusionCol8000-EHU с технологией непрямого адиабатического охлаждения. В решении применяется теплообменник, обеспечивающий охлаждение циркулирующего в ЦОДе воздуха внешним воздухом с улицы. Когда температура на улице становится выше 16°C, включается система распыления воды, обеспечивающая охлаждение воздуха во внешнем контуре. В неблагоприятных для адиабатики условиях дополнительно включается компрессорный (DX) блок, ко-

торый доохлаждает воздух во внутреннем контуре. В уже реализованных проектах использование системы позволило достичь PUE менее 1,15.

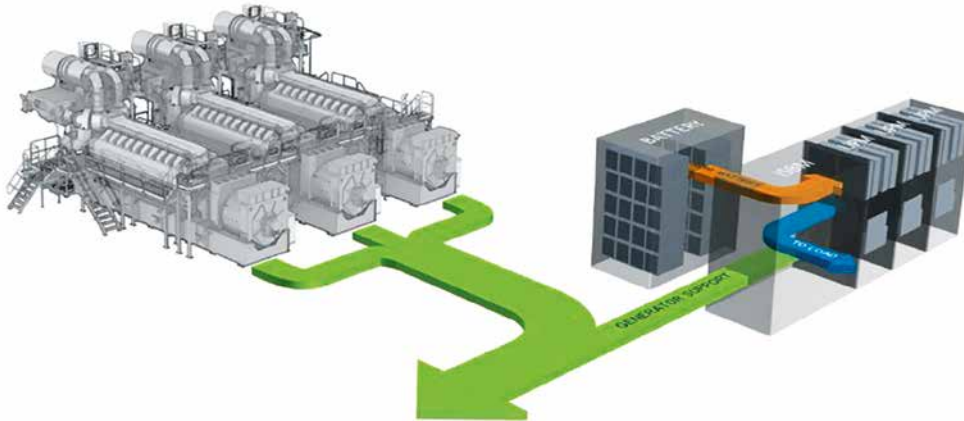
Решение адаптировано для работы при наружных температурах до –40°C. Оно может компоноваться шкафами с литий-ионными АКБ, обеспечивающими непрерывное охлаждение даже в отсутствие ИБП. Это дает немалую экономию. Кроме того, система накопления энергии на базе АКБ позволяет снизить пиковую мощность, потребляемую системой охлаждения от внешней сети, что уменьшает расходы на оплату электроэнергии.

Система FusionCol8000-EHU поставляется как интегрированный блок, собранный на заводе, благодаря чему выигрыш во времени при реализации проекта ЦОДа, по словам Александра Колесникова, главного менеджера по решениям ЦОД компании Huawei, может достигать 90 дней.

Rittal предложила технологию прямого контактного испарительного охлаждения, которую можно назвать шагом в завтра. Эта технология, разработанная партнером Rittal компанией ZutaCore, основана на двухфазном прямом охлаждении процессора с применением газа Novac 7000.



◀ Работа FusionCol8000-EHU с использованием адиабатического охлаждения



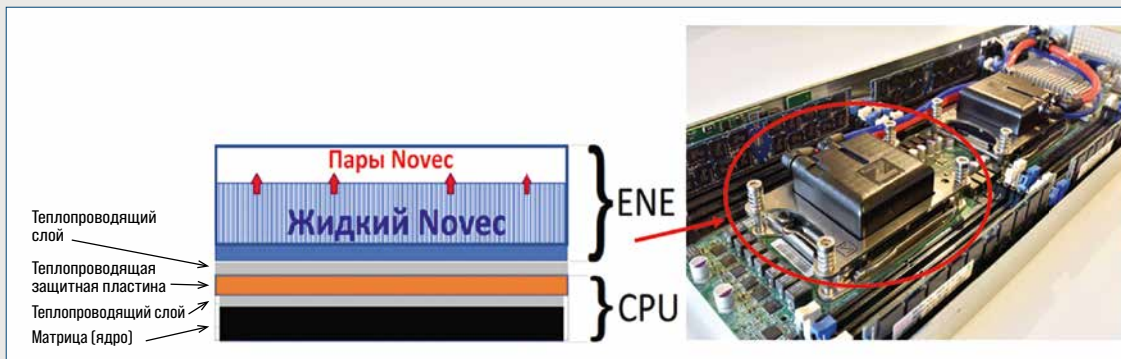
◀ **Рис. 4.**
Использование ИБП ЦОДов не только для питания ИТ-нагрузки, но и для стабилизации работы внешней электросети

Зарабатываем на энергосистеме ЦОДа

Интересную идею о том, как система электропитания ЦОДа позволит его владельцу заработать, выдвинул Олег Иванов, руководитель инженерно-технического отдела компании Eaton. По его данным, сейчас ЦОДы используют 1–2% общемирового количества генерируемого электричества, но к 2030 г. этот показатель может увеличиться до 10%.

ЦОДы становятся все более заметными участниками электроэнергетического рынка. Вместе с тем, как показывает опыт Европы, стабильность работы электросетей из-за активного вне-

дрения систем альтернативной энергетики снижается. ЦОДы, являясь энергоемкими объектами, могут помочь эту стабильность повысить, поскольку их огромная запроецированная мощность обычно потребляется не полностью. «Энергия, накопленная в АКБ, может отдаваться не только в нагрузку, но и в сеть, стабилизируя отклонения частоты», – считает эксперт Eaton. При этом гибкое управление потоками электроэнергии позволяет всегда использовать полную мощность системы ИБП с учетом резервирования – и для обеспечения работы критической нагрузки, и для поддержки энергораспределительной сети (рис. 4).



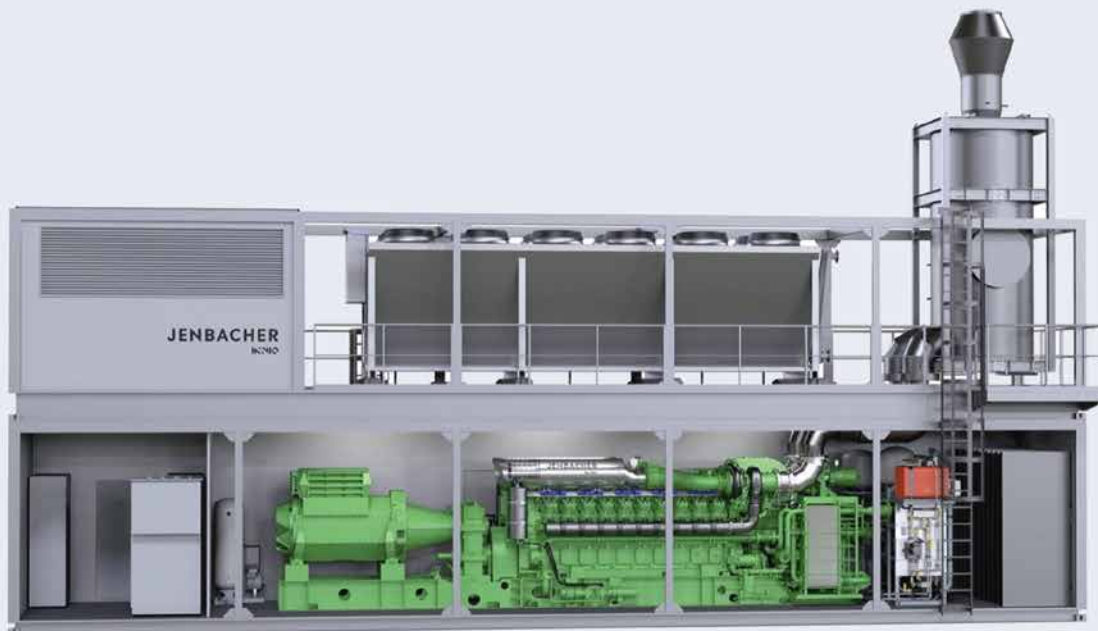
◀ **Принципиальная схема CPU с установленным теплообменником ENE**

Фазовый переход происходит в теплообменнике ENE, установленном непосредственно на процессоре. Поскольку Noves является диэлектриком, даже в случае его утечки ИТ-оборудование повреждено не будет.

Александр Ежов, менеджер по системам контроля микроклимата Rittal, обосновал необходимость подобных систем очень просто. По его оценке, классическое воздушное охлаждение позволяет снять с процессора не более 200 Вт тепла. А уже в нынешнем году Intel планирует вывести на рынок новую серию CPU с тепловыделением 400 Вт. Понятно, что без принципиально новых систем охлаждения отвести такое количество тепла невозможно. И ZutaCore уже тестирует теплообменник ENE для нового процессора.

Mitsubishi Electric разработала HPC (Hydronic Plant Connect) – инновационную систему управления оборудованием для охлаждения дата-центров. Она позволяет оптимизировать управление наружными и внутренними блоками чиллерной системы MENITS без дополнительного оборудования. Логика управления HPC выбирает наилучшее сочетание уставки чиллеров, производительности насосов, вентиляторов и клапанов внутренних кондиционеров для достижения максимальной эффективности системы. При переходе на логику HPC (с логики управления предыдущего поколения) годовое энергопотребление системы охлаждения дата-центра в Милане сократилось примерно на 20%.

Рис. 5.
 Генератор
 на основе газо-
 поршневого
 двигателя с
 абсорбционным
 чиллером ▶



Это не умозрительная идея. Необходимая для ее претворения в жизнь технология EnergyAware уже реализована в ИБП Eaton (Eaton 93PM, Power Xpert 9395P). Более того, она используется в штаб-квартире Eaton в Ирландии, а также в ряде ЦОДов в Финляндии, Швеции и Норвегии. В США совместно с Microsoft проводится пилотное тестирование. АКБ в такую систему могут устанавливаться как свинцово-кислотные, так и литий-ионные.

«Раньше электроэнергия была товаром и считалась потребленной сразу после поставки – продали и забыли. Сегодня возможности хранения и использования электроэнергии между максимумами потребления превращают ее в актив. Хранилища электроэнергии помогают системе быть более гибкой, – рассуждает О. Иванов. – В будущем энергосистемы зданий и ЦОДов, быстро отвечающие на инциденты в распределительной сети, будут служить активами для внедрения технологий генерации возобновляемой энергии».

Идею использования энергетических систем ЦОДов для внешних электросетей развивает Евгений Чурдалёв, старший менеджер по продажам газопоршневых двигателей компании INNIO Jenbacher. При многочисленных преимуществах систем генерации на базе таких двигателей – высокой надежности, сниженных выбросах, низкой себестоимости вырабатываемой энергии – стоят они дороже традиционных ДГУ. Поэтому, считает эксперт INNIO Jenbacher, держать их только в качестве резервных генераторов для да-

та-центра невыгодно. Один из вариантов – задействовать в качестве основного источника энергии ЦОДа, другой – в качестве резервного, но при этом включать в периоды пиковых нагрузок (два раза в будний день примерно по часу) для подачи электричества во внешнюю сеть.

Как утверждает Е. Чурдалёв, российское правовое поле позволяет станциям с установленной мощностью до 25 МВт работать в полупиковом режиме на розничном рынке электроэнергии. Такой режим уже используют более десятка заказчиков INNIO Jenbacher. По оценкам, которые приводит Е. Чурдалёв, станция мощностью 10 МВт будет приносить ЦОДУ ежегодный доход не менее 140 млн руб.

Главная особенность систем INNIO Jenbacher, позволяющая эффективно использовать их в подобных сценариях, – высокая скорость запуска в работу (до 45 с). Естественно, что приоритет такой системы в ЦОДе – это надежное электропитание критической нагрузки объекта. Дополнительным преимуществом является возможность оснащения станций абсорбционными чиллерами, которые за счет сбрасываемого тепла будут генерировать необходимый ЦОДам холод (рис. 5).

Понятно, что в России использование обратной генерации ставит ряд нормативных вопросов. Кроме того, далеко не все владельцы ЦОДов согласятся на то, чтобы ресурсы их энергосистемы задействовались для внешних потребителей. Но в целом идеи, предложенные Eaton и INNIO Jenbacher, достойны внимания и детального изучения. **ИКС**

Rittal – The System.

Faster – better – everywhere.

Рядные фреоновые кондиционеры LCP DX

Уникальные технологии в компактном корпусе



- Мощность охлаждения до 25 кВт при опорной площади 0,36 м²
- Инверторный компрессор. EC-вентиляторы и EEV
- Модели DX/FC со встроенным гидромодулем

Реклама

ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

IT INFRASTRUCTURE

SOFTWARE & SERVICES

FRIEDHELM LOH GROUP

www.rittal.ru



Рядное фреоновое охлаждение: до 69 кВт холода с квадратного метра

Компания Rittal предлагает полную гамму высокотехнологичных и надежных решений для обеспечения бесперебойного функционирования ЦОДа, включая системы контроля микроклимата.

Информационные технологии глубоко проникли в нашу жизнь, и речь идет не только о личных интернет-страницах или онлайн-ресурсах предприятий. Повсеместная цифровизация, внедрение новейших технологий, автоматизация производств, электронный документооборот, а в последние два года еще и массовый перевод сотрудников на удаленный режим работы – все это приводит к тому, что объем генерируемых данных непрерывно растет и требуется все больше ресурсов для их передачи, хранения и обработки. Часть предприятий для этих целей строят собственные центры обработки данных, часть пользуются услугами коммерческих.

Удачная идея

Глобальные ИТ-производители стремятся удовлетворить растущий спрос на вычислительные мощности, выпуская все более производительное серверное оборудование. Но, как известно, чем больше мощности – тем больше тепла, а классическая схема охлаждения с расстановкой кондиционеров шкафного типа по периметру машзала ЦОДа и подачей охлажденного воздуха через пространство фальшпола хорошо работает при тепловыделении до 6 кВт с одной ИТ-стойки. Связано это с потерями производительности из-за большого количества препятствий и высокого сопротивления подпольного пространства, неконтролируемого теплообмена и перетоков между холодными и горячими потоками воздуха.

Поэтому еще в 2008 г. компания Rittal, опираясь на свой 30-летний опыт разработки и производства си-

стем контроля микроклимата для промышленности, представила первый в мире рядный кондиционер для ИТ-оборудования, получивший название Liquid Cooling Package. Это была настоящая революция в мире систем ИТ-охлаждения: в отличие от обычных шкафных кондиционеров, LCP устанавливался непосредственно в ряду серверных стоек, в качестве хладагента использовалась вода, а ширина его составляла всего 300 мм. Отказ от использования пространства фальшпола в качестве воздуховода и ощутимое уменьшение расстояния между серверным оборудованием и теплообменником позволило минимизировать вышеописанные теплотери и увеличить показатель отводимого со стойки тепла до 12 кВт. Идея рядного кондиционера оказалась настолько удачной, что все ведущие производители начали разработку и выпуск подобных решений.

Современные рядные водяные кондиционеры LCP CW компании Rittal имеют холодопроизводительность до 53 кВт в корпусе с основанием всего 300 x 1200 мм, а задействование режима фрикулинга в чиллерах позволяет ощутимо снизить затраты на электроэнергию в холодное время года. Минусом использования воды в качестве теплоносителя является относительно высокая стоимость машин для ее охлаждения – чиллеров: для малых и средних ЦОДов это решение оказывается дороже классического фреонового охлаждения. В связи с этим в 2011 г. компания Rittal выпустила фреоновую версию рядного кондиционера с выносным конден-

саторным блоком – Liquid Cooling Package DX. Это решение идеально подходит для отвода излишков тепла в небольших серверных и в крупных ЦОДах при невозможности применения воды или ее растворов.

Внутри LCP DX

Стандартная комплектация кондиционеров LCP DX компании Rittal уже включает инверторный компрессор и электронно-коммутируемые вентиляторы (ЕС-технология). Это существенно экономит электроэнергию, дает возможность плавно регулировать производительность, минимизировать пусковые токи и защищать электродвигатели от перегрузки, что значительно увеличивает срок эксплуатации. Необходимый и важный элемент любого фреонового контура – расширительный вентиль. Все LCP DX осна-



Виброгасящая вставка на линии нагнетания



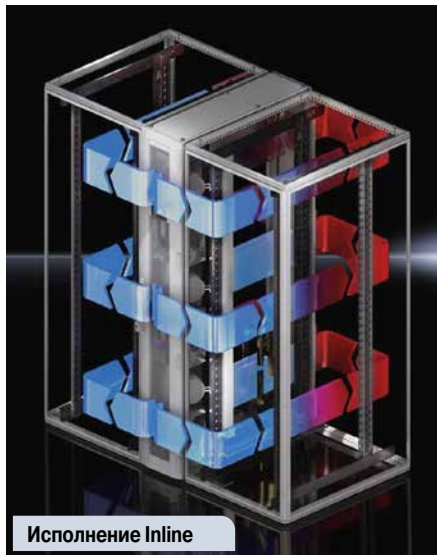
Александр Ежов, менеджер по продукции «Системы контроля микроклимата», Rittal

щаются только электронным расширительным вентилем (ЭРВ): использование цифровых датчиков и многопозиционной электромагнитной катушки делает его гораздо надежнее и позволяет максимально быстро и точно регулировать подачу фреона в испаритель. Графический дисплей высокого разрешения, сетевая SNMP-карта, поддержка автоматического рестарта и групповой работы (до восьми кондиционеров) также входят в стандартную поставку.

Компания Rittal использует не только передовые решения, но и свой промышленный опыт. Например, система виброизоляции компрессора включает в себя не только классические виброизолирующие опоры и хомуты, но и виброгасящую вставку («анаконду») на линии нагнетания. Она необходима для поглощения микропульсации фреона – основной причины разгерметизации фреонового контура в конденсаторном блоке (эффект «перетирания» медных трубок о стенки и усилители корпуса). При этом сама линия нагнетания имеет форму маслоподъемной петли, что упрощает оборот компрессорного масла по фреоновому контуру. Основной контроллер и узел электроподключения размещены в защищенном боксе в верхней части, а вводы имеют герметичное исполнение. На испарителе установлено шесть датчиков температуры воздуха, по три на входе и выходе – это позволяет плавно регулировать производительность по зонам высоты, а также резервировать сами датчики на случай выхода из строя одного из них. Стоит отдельно отметить, что главные элементы контроля и управления (основной контроллер, дисплей, датчики, контроллер EEV и драйвер управления компрессором) разрабатываются и поставляются одним производителем – это гарантирует полную совместимость, высокую надежность и отказоустойчивость. Компрессорная группа во всех LCP DX находится во внутреннем блоке: в отличие от решений с ее выносом в наружный блок, это позволяет смягчить условия эксплуатации и максимально продлить срок службы, а сам конденсатор сохраняет низкий уровень шума, компактность и малый вес.

Готовые решения для любых задач

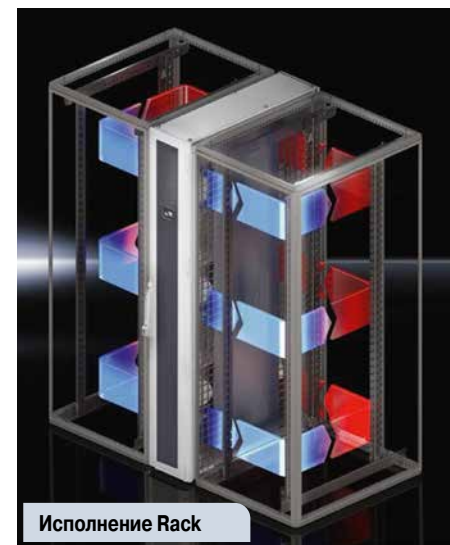
Компания Rittal выпускает рядные кондиционеры LCP DX с холодильной мощностью 12, 20 и 25 кВт с шириной корпуса 300 мм в исполнении Inline



(охлаждение ряда с использованием системы отделения коридора) или Rack (непосредственное охлаждение присоединенных стоек). Холодильную мощность 35 кВт может обеспечить модель в корпусе 600 мм и исполнении Inline. Для всех моделей доступны три варианта наружного блока, самый популярный – низкотемпературный конденсатор с модулем зимнего комплекта (готовый к подключению бокс с установленными необходимыми компонентами). Также доступна гибридная модель LCP DX/FC на 35 кВт, которой для работы не требуется чиллер: внутренний блок снабжен встроенным гидромодулем с инверторным насосом, а для охлаждения воды используется соответствующий конденсатор, совмещающий фреоновый и водяной контуры.

Для нестандартных требований Rittal предлагает различные опции. Самая популярная – это ультразвуковой увлажнитель воздуха: при потреблении всего 40 Вт он производит 0,5 кг холодного пара в час. Это фактически не влияет на энергопотребление

и не уменьшает полезную холодильную мощность, при этом сам процесс увлажнения начинается сразу по запросу, а не после того, как вода достаточно нагреется и закипит. Также доступен насос конденсата (если прокладка дренажной линии под уклоном невозможна), воздушный фильтр с датчиком контроля загрязнения (многоразовые фильтры промываются во-



дой), подогрев воздуха и система осушения. Возможен заказ специзделия: например, с увеличенной высотой для установки в ряду стоек 47 или 52U, покраской корпуса в необходимый цвет, двойным вводом питания и АВР.

Высокая мощность в компактном корпусе

Возможность легко наращивать мощность ЦОДа – еще одно весомое преимущество LCP DX. При расширении или модернизации парка ИТ-оборудования достаточно установить дополнительные рядные кондиционеры (увеличение длины ряда) или заменить имеющиеся на более производительные (с такими же габаритами). При этом показатель холодопроизводительности LCP DX достигает 69 кВт на 1 кв. м занимаемой площади (опорная площадь LCP DX мощностью 25 кВт составляет всего 0,36 кв. м).



**ООО «Риттал», 125252, Москва,
ул. Авиаконструктора Микояна, 12, БЦ «Линкор», 4 этаж
тел. (495) 775-0230
info@rittal.ru, www.rittal.ru**

Бесперебойное электропитание ЦОДов: тенденции до 2025 года

Системы бесперебойного питания для дата-центров постоянно развиваются. Новые технологии позволяют использовать различные подходы к организации энергетических инфраструктур. Но будут ли ИБП будущего соответствовать меняющимся требованиям операторов?



Ронда Асьерто, вице-президент, Пол Джонсон, технический консультант, Uptime Institute

Развитие энергетической инфраструктуры дата-центров в ближайшие годы будет определяться необходимостью снижения капитальных затрат без повышения рисков, требованиями регуляторов и меняющимися запросами клиентов. Все больше операторов ЦОДов стремятся к повышению эффективности, адаптируемой отказоустойчивости и интегрированной автоматизации. Новые аккумуляторные технологии (и возобновляемые источники энергии) будут использоваться все шире, особенно в ЦОДах, поддерживающих очень высокие критические нагрузки, а таких объектов становится все больше.

В этой статье рассматриваются лишь потенциальные изменения, связанные с распределенными системами бесперебойного питания и ИБП среднего напряжения, а также со способами масштабирования, эффективного обслуживания и удаленного мониторинга централизованных систем ИБП.

Выводы основаны на интервью с представителями 21 оператора ЦОДов (коммерческих, т.е. предоставляющих услуги colocation, облачных, телекоммуникационных и корпоративных), восьми компаний, занимающихся обслуживанием ЦОДов и инженерными системами, а также с восемью консультантами Uptime Institute. В основном они касаются крупных ЦОДов с мощностью, выделенной для ИТ-оборудования, не менее 1 МВт (средняя мощность объектов в нашем исследовании – около 65 МВт). Для небольших периферийных (edge-) ЦОДов выводы могут быть иными.

Распределенные системы бесперебойного питания

Некоторые крупные ЦОДы используют распределенную систему бесперебойного питания – например, защиту электропитания с помощью аккумуляторных батарей, установленных в сер-

верных стойках или в рядах стоек. Такой подход предусматривается в альтернативных (традиционным) проектах инфраструктуры, в частности в Open Compute Project. Подобные «открытые» архитектуры позволяют операторам достичь большей эффективности по нескольким направлениям. Некоторые ЦОДы смогли добиться 25%-ного снижения капитальных затрат по сравнению с традиционным централизованным подходом только за счет электросетевой топологии.

Учитывая очевидные стоимостные преимущества этого подхода и его поддержку некоторыми крупными операторами ЦОДов, широкое использование распределенной архитектуры долгое время считалось неизбежным. Однако пока количество внедрений сильно отстает от ожиданий отрасли. Как показало наше исследование, внедрение распределенного подхода может ускориться, но незначительно: перейти на распределенную топологию в своих основных ЦОДах или расширить ее использование к 2025 г. планирует только пятая часть опрошенных операторов. Большинство этих операторов управляют облачными дата-центрами. Небольшое число colocation-ЦОДов также ожидают более широкого применения таких архитектур. Чаще всего побуждают к этому совершенствование технологий аккумуляторных батарей (литий-ионные АКБ), стандартизация и удовлетворение запросов клиентов (как правило, крупных). Два респондента заявили, что в перспективе батареи, скорее всего, перестанут быть частью системы ИБП и начнут встраиваться в серверы, что обусловит переход на распределенную архитектуру бесперебойного питания.

Другие причины ожидаемого роста популярности распределенных систем бесперебойного питания:

- возможность лучше адаптировать мощности ИБП к изменениям плотности мощности (колебаниям нагрузки) в стойке;

Публикуется с разрешения Uptime Institute.

- повышение доступности и сокращение среднего времени устранения неисправностей (хотя ИБП в распределенной системе могут быть статистически менее надежными, но быстрота устранения неисправностей повышает общий показатель готовности);

- возможность управлять батареями и оптимизировать их работу на индивидуальной основе.

Не все облачные ЦОДы, эксплуатирующие распределенные системы бесперебойного питания сегодня, планируют расширять их использование – 43% таких операторов не имеют подобных планов. Среди провайдеров colocation таковых 72%. Большинство участников нашего исследования вообще не собираются внедрять распределенные системы до 2025 г.

У части операторов облачных ЦОДов на распределенные системы приходится 10–20% общего комплекса систем ИБП на объектах, однако у одного оператора эта доля составляет 50%. Никто не ожидает, что указанные пропорции к 2025 г. изменятся.

Каковы же препятствия на пути внедрения или более широкого использования распределенных систем бесперебойного питания? Сдерживающих факторов множество, наиболее распространенные – пожелания потребителей услуг colocation. Несколько крупных операторов colocation заявили, что их клиенты не хотят, чтобы они применяли такие системы защиты электропитания. У этих операторов много небольших клиентов, и централизованная схема предпочтительна, поскольку она позволяет обеспечивать защищенным электропитанием нагрузку нескольких клиентов. Кроме того, представители разных групп операторов выразили опасения относительно стоимости и безопасности новых технологий аккумуляторных батарей, используемых в децентрализованных подходах.

Другие названные недостатки распределенных систем:

- Размещение систем ИБП в машзалах может вызвать проблемы с тепловой нагрузкой. Кроме того, такие системы занимают ценное пространство, которое можно сдать в аренду.

- Размещение систем ИБП в машзалах может создать проблемы с безопасностью. Например, обслуживающему такие системы персоналу может быть отказано в доступе в зал из-за критически важных ИТ-систем клиентов, вследствие чего техническое обслуживание не будет выполнено вовремя.

- Распределенные системы более сложны, менее гибки, и их труднее обслуживать.

Похоже, что по крайней мере в следующие несколько лет для большинства групп наших респондентов опасения заказчиков будут переве-

шивать все преимущества распределенной архитектуры ИБП. Этот подход останется предпочтительным вариантом для относительно небольшого числа крупных операторов, в основном управляющих облачными ЦОДами.

ИБП среднего напряжения

Сегодня большинство централизованных трехфазных ИБП работают при напряжении 380 В. Системы ИБП, работающие при более высоком напряжении, могут обеспечить большую эффективность. При использовании ИБП среднего напряжения (6–20 кВ) можно снизить капитальные и эксплуатационные расходы, поскольку электрические токи и, следовательно, потери ниже, а кабели могут иметь меньшее поперечное сечение (диаметр). Системы ИБП среднего напряжения уменьшают потребность в сопутствующих компонентах (распределительных устройствах). Кроме того, их можно размещать дальше от машзалов (например, на подстанции или в специальном помещении), чем системы низкого напряжения.

Однако подавляющее большинство участников нашего исследования заявили, что вряд ли внедрят ИБП среднего напряжения к 2025 г. Их нежелание обусловлено неясностью в вопросах общей стоимости владения (ТСО) и эффективности. Тем не менее двое респондентов, которые, может быть, внедрят такие ИБП, ожидают от них снижения ТСО. Конкретные доводы в пользу ИБП среднего напряжения включают:

- уменьшение занимаемой площади;
- возможность большего удаления ИБП от ИТ-нагрузки;
- возможность поддерживать вычисления высокой плотности и изменяющиеся нагрузки, в частности приложения искусственного интеллекта (ИИ).

Централизованные ИБП

Централизованные трехфазные ИБП уже давно предпочтительны для большинства крупных (с общей мощностью ИБП 1 МВт или более) корпоративных и colocation-ЦОДов. Считается, что централизованные системы обеспечивают более высокий уровень надежности по сравнению с модульными или распределенными решениями благодаря наличию лишь одного статического переключателя. В модульных или распределенных решениях используются несколько небольших статических переключателей, а это означает, что неисправности могут «проходить» через них – проблема, весьма существенная для многих операторов крупных ЦОДов. (При этом на объектах мощностью менее 1 МВт модульные и распределенные системы ИБП часто дешевле и проще в управлении.)

Централизованные системы ИБП также быстро и легко развертываются в крупных ЦОДах и часто предпочтительны, когда ожидается быстрое заполнение ИТ-залов. Однако операторы не считают, что их покупка и эксплуатация обходятся недорого. И, как обсуждается ниже, у них есть свои проблемы.

Централизованные ИБП, вероятно, будут по-прежнему доминировать в ЦОДах с ИТ-мощностью 1 МВт и более, особенно в крупных корпоративных и colocation-ЦОДах – по крайней мере в следующие пять, а скорее всего, и 10 лет. Отчасти это объясняется тем, что новации в технологиях ИБП обычно появляются медленно и так же медленно принимаются заказчиками. Многие операторы и клиенты colocation-ЦОДов не склонны что-либо менять, когда речь идет о хорошо зарекомендовавших себя критически важных компонентах.

Возможно, самые большие изменения в системах ИБП будут связаны с аккумуляторными технологиями – хотя, как отмечалось выше, новые подходы, в частности использование литий-ионных АКБ, по-прежнему вызывают озабоченность и скептицизм.

Болевые точки

Как уже говорилось, централизованные трехфазные ИБП устанавливаются в большинстве ЦОДов, но они не лишены недостатков (рис. 1). Прогнозируется, что многие из существующих проблем к 2025 г. решены не будут. Также вероятно возникновение новых.

Основные болевые точки ИБП – аккумуляторные батареи, надежность и безопасность. С этими проблемами сталкиваются дата-центры всех типов. Как показало наше исследование, надежность и безопасность продуктов особенно беспокоят операторов облачных и colocation-ЦОДов, а также операторов связи. Кроме того, у многих возникают сложности с рабочими/выходными характеристиками, обслуживанием и вводом в эксплуатацию.

Наиболее распространенные жалобы на АКБ сегодня связаны с необходимостью их частого технического обслуживания, готовностью и работоспособностью (несмотря на заявления производителей). Отсутствие коммерчески доступных средств интеграции батарей также является проблемой для некоторых респондентов.

Забегая вперед, скажем, что многие ожидают проблем и с литий-ионными батареями, в том числе с установкой, пожарной безопасностью, мониторингом и проверкой состояния. Те, кто уже развернул такие системы, готовятся к возможным высоким затратам в конце срока их службы, в частности из-за отсутствия отработанных механизмов утилизации этих батарей.

Сегодняшние опасения относительно надежности и безопасности продуктов обусловлены в основном сложностями обеспечения непрерывности обслуживания и увеличением числа отключений. И эти проблемы, по мнению большинства, сохранятся до 2025 г.

Рис. 1. Основные болевые точки централизованных трехфазных ИБП в 2020–2025 гг. (приведено число ответов) ▼



Источник: Uptime Institute Intelligence, 2020 (n = 32)

Барьеры, препятствующие внедрению ИБП среднего напряжения



Совокупная стоимость владения, в том числе высокие первоначальные затраты и предполагаемое отсутствие финансовой отдачи. Более высокие сопутствующие затраты включают в себя покупку генератора среднего напряжения (большие размеры оборудования плюс затраты на установку) или дополнительного повышающего трансформатора.

Удаление ИБП от нагрузки. Установка ИБП (низкого напряжения) и батарей как можно ближе к нагрузке означает меньшую вероятность сбоя на линии распределения питания. ИБП среднего напряжения располагается дальше от серверного зала, что повышает вероятность таких сбоев.

Риски для клиентов. Несколько крупных операторов colocation-ЦОДов сообщили, что,

по мнению многих их клиентов, установка ИБП среднего напряжения может повысить риски. Большинство привыкло видеть традиционный статический ИБП рядом с машзалом ЦОДа, и другой вариант, к тому же удаленный от ИТ-нагрузки, рассматривают как дополнительный риск.

Риски, связанные с безопасностью, в том числе при работе с более высоким напряжением. Один респондент ссы-

Некоторые заказчики сталкиваются с высокой частотой отказов, в том числе вентиляторов ИБП, а в старых моделях – инверторов. Один оператор заявил, что ИБП вышел из строя при работе на полную мощность, выдав при этом сообщение о «многочисленных сбоях внутренних компонентов». Было высказано мнение, что общий высокий спрос на системы ИБП в последние несколько лет мог привести к тому, что заводские испытания не проводятся в полном объеме, поэтому дефекты производства, сборки или настройки могут остаться невыявленными до отгрузки продукции потребителю.

Некоторые участники нашего исследования выразили обеспокоенность надежностью систем ИБП, которые к 2025 г. будут близки к окончанию срока службы. Их также волнует доступность постоянной поддержки продуктов со стороны производителей. Другие обеспокоены тем, что к 2025 г. централизованные ИБП могут оказаться неспособными адекватно поддерживать приложения ИИ и другие сильно изменяющиеся рабочие нагрузки. Это может привести к тому, что в пиковое время ИТ-мощности нельзя будет задействовать полностью из-за недостаточной мощности систем бесперебойного электропитания – отчасти из-за плохого управления их рабочей нагрузкой. Повышение эффективности, гибкости и уменьшение размеров – это направления улучшения ИБП, на которые рассчитывают наши респонденты.

Семь участников нашего исследования, представляющие ЦОДы разных типов в разных регионах, заявили, что не сталкиваются с проблемами при эксплуатации систем ИБП, и пятеро из них не ожидают, что проблемы возникнут в ближайшие пять лет. Двое других полагают, что к 2025 г. возникнут проблемы с батареями, а также с надежностью продуктов по мере их старения.

ляется на риск более строгих нормативных требований в будущем, которые могут ограничить возможность использовать ИБП среднего напряжения.

Масштабируемость. Несколько респондентов говорят, что их нагрузки недостаточно велики (и не будут достаточно велики в будущем), чтобы оправдать установку ИБП среднего напряжения. Один оператор заявил, что такие ИБП не подходят для colocation-ЦОДов, потому что они не столь масштабируемы. Системы ИБП низкого напряжения

имеют модули (устройства) меньшей мощности, а значит, их можно масштабировать более точно.

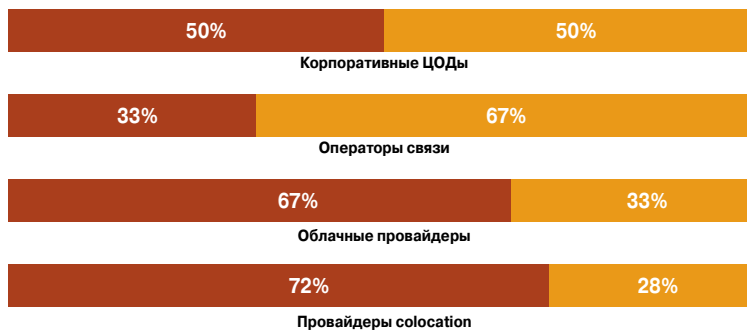
Слишком новая технология. Респонденты говорят, что технология слишком нова и, следовательно, не апробирована. Некоторых останавливает отсутствие достаточного числа успешных внедрений продукта – в частности, невозможность сравнить эффективность новых систем, занимаемую ими площадь, надежность и доступность.

Выбор поставщика. Некоторые респонденты обеспокоены огра-

ниченностью числа производителей ИБП среднего напряжения, что может негативно повлиять на стоимость и доступность продуктов.

Дефицит специалистов. Обычно упоминают трудности с поиском лицензированных электриков по среднему напряжению во многих странах. Ограниченная доступность обученного персонала поставщика также вызывает озабоченность, как и ограниченная локальная доступность и длительные сроки поставки запасных частей.

■ Добавление новых устройств (конструктивов) ■ Добавление емкости в уже используемые конструктивы



Источник: Uptime Institute Intelligence, 2020

Масштабирование

Как операторы ЦОДов различных типов будут к 2025 г. масштабировать свои централизованные трехфазные системы бесперебойного питания? Как будет обеспечиваться резервирование: за счет добавочной емкости внутри конструктивов ИБП или за счет установки новых устройств?

Опрошенные операторы облачных и colocation-ЦОДов предпочтут масштабировать систему за счет установки новых устройств, в то время как большинство операторов связи намерены увеличить емкость уже имеющихся ИБП (рис. 2).

Расширение за счет добавления новых устройств рассматривается большинством операторов ЦОДов как способ снизить риск. Этот подход также может повысить безопасность на некоторых объектах, поскольку позволяет избежать проведения работ в уже находящихся в эксплуатации устройствах. Еще одна причина, по которой операторы выбирают добавление новых устройств, – экономическая эффективность. Такой выбор помогает уменьшить необходимость исходного перераспределения емкости ИБП: каждый ИБП имеет свой блок батарей, а

▲ Рис. 2. Предпочтительные способы масштабирования централизованных трехфазных ИБП к 2025 г.

при наращивании емкости уже установленных ИБП приходится расширять его комплекс АКБ или переразмеривать его с самого начала. Кроме того, установка дополнительных устройств считается наиболее быстрым способом наращивания мощности.

Однако большинство респондентов, которые предпочли бы добавлять модули в существующие конструктивы ИБП, считают менее рискованным свой путь. Расширение в рамках установленных конструктивов они рассматривают как более отказоустойчивое (следовательно, с более низким риском простоя), поскольку избыточность реализуется на уровне одного устройства ИБП. Кроме того, по их мнению, модульный подход позволяет лучше адаптироваться к увеличению ИТ-нагрузки. Сторонники использования модульных ИБП отмечают и быстроту развертывания, в частности потому, что все кабели, конструктивы (шкафы) и распределительные устройства устанавливаются сразу при начальной инсталляции ИБП.

Новые высокоэффективные режимы

КПД большинства централизованных трехфазных ИБП сегодня составляет 94–96% в обычном рабочем режиме. Режим экономии (экорезжим с подачей «неочищенного» питания через байпас ИБП) отключает процесс двойного преобразования, что обеспечивает более высокий КПД – как правило, до 98%.

В последние годы появились новые высокоэффективные усовершенствования экорезжима. Они позволяют активно управлять преобразованием мощности путем устранения искажений, но с меньшими потерями (при сохранении того же уровня защиты питания и того же уровня резервирования за счет АКБ).

Однако более половины (60%) участников исследования заявили, что вряд ли к 2025 г. перейдут на новые высокоэффективные режимы для централизованных трехфазных систем ИБП, поддерживающих только ИТ-нагрузку – в отличие от систем, поддерживающих механиче-

скую нагрузку или сочетание ИТ- и механической нагрузки (рис. 3).

Наибольший консерватизм в отношении новых режимов выказали операторы colocation- и корпоративных ЦОДов. Новые высокоэффективные режимы основаны на прямом соединении между входными и выходными клеммами питания (через дроссель или переключающее устройство), но это устраняет гальваническую развязку, обеспечиваемую двойным преобразованием, а значит, нагрузка может подвергаться негативным воздействиям, например, из-за молнии или скачков напряжения. Несколько крупных операторов colocation-ЦОДов заявили, что отсутствие такой развязки недопустимо для многих их клиентов. А один оператор отметил, что даже после заводских испытаний, продемонстрировавших успешную работу ИБП при переключении различных режимов, клиенты по-прежнему предпочитают полноценное двойное преобразование.

Также многих респондентов останавливает общее нежелание быть пионером внедрения новых технологий. Кроме того, они опасаются относительно ограниченного выбора производителей, поддерживающих такие технологии.

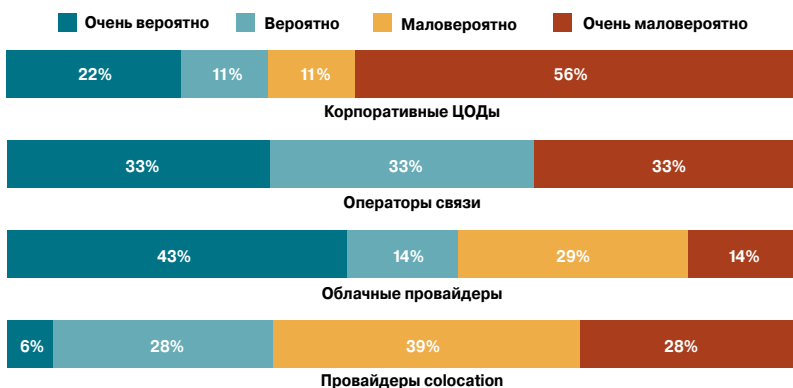
Один респондент указал на недостаточную уверенность в надежной защите электропитания при использовании новых режимов, когда не обеспечивается независимость нагрузки от входных напряжения и частоты (режим VFI) или только напряжения (режим VI). Другой отметил, что многие серверы чувствительны к напряжению питания и требуют наличия источника, осуществляющего его очистку. Операторов ЦОДов беспокоит, что сбои в работе ИТ-серверов, вплоть до отключения, могут произойти незаметно, что серьезно повлияет на их бизнес.

Облачные операторы и операторы связи, скорее всего, в будущем перейдут на высокоэффективные режимы ИБП. Основным стимулом является экономическая эффективность, включая повышение эффективности энергопотребления и снижение общих затрат на электроэнергию.

Удаленный мониторинг с обслуживанием на основе состояния

Некоторые производители ИБП запустили службы удаленного мониторинга для систем ИБП, которые включают – или скоро будут включать – услуги технического обслуживания на основе состояния оборудования. Но большинство (65%) участников нашего исследования заявили, что к 2025 г. их организации вряд ли будут прибегать к таким сервисам (рис. 4), причем как для своих основных ЦОДов (с ИТ-мощностью 5 МВт и более), так и для распределенных edge-ЦОДов (с ИТ-мощностью 200 кВт и более).

Рис. 3. Вероятность использования новых высокоэффективных режимов ИБП к 2025 г. ▼



Источник: Uptime Institute Intelligence, 2020

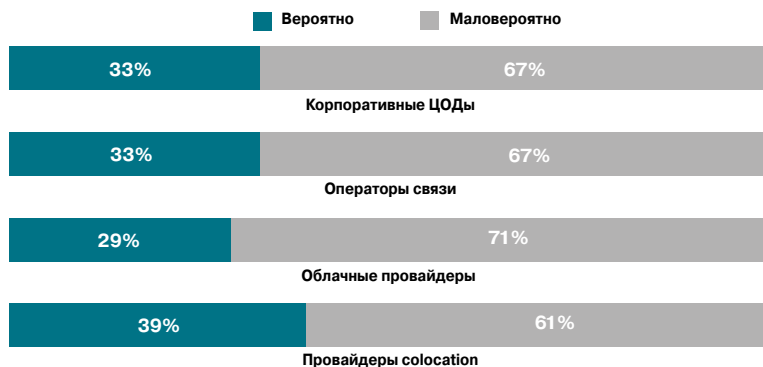
Основной сдерживающий фактор – вопросы безопасности, особенно для операторов облачных и корпоративных ЦОДов. Они говорят о том, что предоставление доступа к критически важному оборудованию непосредственно онлайн-службе (и облаку) производителя сопряжено с техническими и коммерческими рисками. Большинство из них обеспокоены недостаточной защитой, обеспечиваемой межсетевыми экранами, потенциальными брешами кибербезопасности и ситуациями, когда злоумышленники требуют выкуп.

Операторы colocation-ЦОДов, особенно в отраслях с высоким уровнем регулирования (например, финансы и здравоохранение), указали на риск, воспринимаемый клиентами. Преимущества предлагаемых услуг не перевешивают потенциальную потерю доверия клиентов. Одни операторы colocation-ЦОДов опасаются потенциально недостаточной безопасности передачи данных с оборудования на площадке дата-центра в облако производителя. Для других важно обеспечить надежную работу межсетевого экрана и защиту от возможного несанкционированного доступа в систему управления.

Несколько опрошенных предпочли бы использовать собственную систему мониторинга, чтобы сохранить контроль над системой (и данными) и избежать риска внешнего воздействия. Другие не видят адекватной ценности в мониторинге на основе состояния и считают, что самое лучшее – физический осмотр на месте.

Группа участников нашего исследования, которые, скорее всего, воспользуются услугами удаленного мониторинга от производителя ИБП, включает операторов ЦОДов всех типов, расположенных главным образом в Азиатско-Тихоокеанском регионе и в Северной Америке. Они часто рассматривают техническое обслуживание на основе состояния как более эффективное, чем регулярное (по графику). Некоторые говорят, что техническое обслуживание на основе состояния может потенциально сократить количество вмешательств в систему, снизив вероятность человеческих ошибок. Один представитель корпоративного ЦОДа заявил, что будет использовать удаленные службы, но угроза взлома, скорее всего, заставит ограничить возможности производителя ИБП мониторингом (без доступа к функциям управления).

Предполагая, что проблемы безопасности будут решены, те респонденты, которые, скорее всего, согласятся на использование служб удаленного мониторинга, считают, что они повысят эффективность эксплуатации. Некоторые указывают на преимущества ИИ (и других методов работы с большими данными), лежащих в



Источник: Uptime Institute Intelligence, 2020

основе удаленного мониторинга ИБП. Они рассматривают анализ информации в реальном времени, в том числе с помощью ИИ, как инструмент, позволяющий принимать более обоснованные решения, чем другие подходы, и тем самым снижать риски. Некоторые говорят, что ИИ наиболее эффективен в выявлении проблем до их возникновения, что уменьшает число инцидентов.

Выводы

Наше исследование показало, что операторы ЦОДов, как правило, готовы применять новые подходы к организации энергетических инфраструктур только в том случае, если выгоды явно перевешивают риски (технические или коммерческие). Но иногда подход просто слишком нов и недостаточно проверен, особенно с точки зрения корпоративных и colocation-ЦОДов.

В обозримом будущем (к 2025 г.) системами ИБП среднего напряжения вряд ли будут пользоваться значительно больше ЦОДов, чем сегодня. Распределенным системам бесперебойного питания (с распределенными батареями) также будут отдавать предпочтение лишь относительно немногие (в основном облачные) провайдеры.

Централизованные трехфазные ИБП останутся предпочтительным вариантом для большинства ЦОДов – несмотря на различные проблемы, связанные в том числе с батареями, надежностью и безопасностью.

Если производители смогут адекватно отреагировать на опасения операторов относительно повышенного риска, то, вероятно, новые высокоэффективные режимы работы ИБП (дальнейшее усовершенствование традиционных экорежимов) распространятся более широко. Некоторые операторы ЦОДов заинтересованы в услугах удаленного мониторинга ИБП, включая техническое обслуживание на основе состояния оборудования, но только в том случае, если проблемы безопасности будут решены. Многих останавливает сама новизна и необкатанность этих подходов, но после 2025 г. они уже перестанут считаться новыми. ИКС

▲ Рис. 4. Вероятность использования к 2025 г. служб удаленного мониторинга ИБП с услугами техобслуживания на основе состояния оборудования

Натрий-ион для дата-центров

Натрий-ионные аккумуляторы совершенствуются и со временем могут найти применение в системах резервного питания ЦОДов.

**Николай
Носов**

Сегодня наиболее популярным способом хранения электроэнергии является использование литий-ионных (Li-ion) аккумуляторов. На рынке смартфонов они вытеснили никель-кадмиевые (Ni-Cd) и никель-металлогидридные (Ni-MH) аккумуляторы, успешно конкурируют с свинцово-кислотными на рынке дата-центров, стали незаменимой частью стремительно растущего рынка электромобилей.

Изобретатели литий-ионных батарей заслуженно получили в 2019 г. Нобелевскую премию по химии. Но есть у этих батарей и недостатки. Самый известный – взрывоопасность при коротком замыкании и нарушении герметичности корпуса, из-за чего авиакомпании разрешают провозить небольшие аккумуляторы только в ручной клади, а крупные запрещают совсем.

Другой недостаток – высокая стоимость. Вследствие постоянно растущего спроса и ограниченных запасов на планете лития и кобальта она вряд ли будет снижаться, особенно в свете борьбы с глобальным потеплением и отказом от использования невозобновляемых источников энергии. Ведь на аккумулятор только для одного электромобиля понадобится килограммов десять чистого лития и в два раза больше кобальта. 60% кобальта добывается в одной из самых бедных и нестабильных стран мира – Демократической Республике Конго, причем с применением детского труда, что не улучшает имидж производства.

Новый кандидат в лидеры

Наиболее перспективной заменой литию считается натрий. Цена натрий-ионных аккумуляторов (Na-ion) потенциально ниже из-за широкой доступности солей натрия – их запасы огромны. Сходство основных принципов работы натрий-ионных и литий-ионных аккумуляторов позволяет задействовать уже существующие линии производства. Na-ion-аккумуляторы можно хранить

и транспортировать полностью разряженными, что снижает риски безопасности при перевозках. Другой плюс – использование для производства анодного материала более экологичных материалов, вплоть до пищевых отходов.

Натрий-ионные аккумуляторные элементы состоят из катода на основе натрийсодержащего материала, анода и жидкого электролита, содержащего соли натрия. Во время зарядки ионы натрия извлекаются из катода и встраиваются в анод, в то время как электроны проходят через внешнюю цепь. Во время разряда происходит обратный процесс – ионы натрия извлекаются из анода и повторно интеркалируются в катод, а электроны, проходя через внешнюю цепь, выполняют полезную работу.

Разработка Na-ion-батарей началась в 70-х годах прошлого века, параллельно с литий-ионными, но коммерческие перспективы лучше выглядели у Li-ion. Да и применяемый в коммерческих литий-ионных батареях графит плохо подходил для натрий-ионных батарей, так как он не способен накапливать более крупные ионы натрия. Решающим моментом в развитии Na-ion-батарей стало открытие в 2000 г. возможности накопления ионов натрия в некристаллической структуре – «твердом углероде». Этот материал стал основным претендентом на использование в качестве анода.

Долгое время исследования в области натрий-ионных аккумуляторов шли достаточно вяло, поскольку основной интерес был направлен на литий-ионные. Однако, когда сфера применения последних начала включать столь энергоемкие источники, как электромобили, системы бесперебойного питания ЦОДов и системы компенсации нагрузок в электросетях, стало ясно, что нужна более дешевая альтернатива с доступной базой исходного сырья. Это вызвало резкий рост числа научных работ и технологических стартапов в области Na-ion.

Путь к месту в бизнес-классе

В начале 2015 г. RS2E, французская исследовательская и технологическая сеть, занимающаяся электрохимическим накоплением энергии, в сотрудничестве с Национальным центром научных исследований Франции (CNRS) выпустила первую Na-ion-батарею в формате 18650 (диаметр 18 мм, высота 65 мм, рис. 1).



▲ Рис. 1. Na-ion батарея CNRS

Tiamat (дочерняя компания CNRS), британская компания Faradion Limited и китайская HiNa встали во главе движения по коммерциализации Na-ion батарей. В 2018 г. организованная на базе Института физики Китайской академии наук HiNa разработала низкоскоростной мини-электромобиль с питанием от Na-ion-аккумуляторов. Tiamat в марте 2021 г. сообщила о привлечении 5 млн евро для начала производства натриевых аккумуляторных батарей для гибридных автомобилей. Натрий-ионные батареи Faradion будет применять в мобильных накопителях солнечной энергии английская компания AceOn. Эту технологию планируют использовать в коммерческих целях в странах Африки к югу от Сахары.

Натрий-ионные батареи разрабатываются и в России. Лаборатория материалов для электрохимических процессов химического факультета МГУ запатентовала в 2019 г. анодные и катодные материалы для натрий-ионных батарей. Работы коллектива в этой области вошли в топ-10 научных открытий 2020 г. в России. Свои разработки лаборатория продемонстрировала на форуме «Армия-2021»: к такой батарее была подключена загорающаяся световая рамка (рис. 2).



▲ Рис. 2. Na-ion батарея МГУ

Представитель лаборатории Григорий Лакиенко пояснил нашему изданию, что считает перспективным использование натрий-ионных батарей для сохранения энергии солнечных электростанций или в качестве резервного источника питания в дата-центре. Хотя натрий-ионный аккумулятор дешевле литий-ионного аналогичной мощности, но по массогабаритным характеристикам уступает последнему. Поэтому в мобильной электронике у Li-ion пока нет конкурентов, но в больших комплексах батарей масса не так критична и цена становится важнее. Исполнительный директор по исследованиям Uptime Institute Энди Лоуренс отмечает, что они могут заменить и ДГУ: «Уже появились альтернативные технологии, которые могли бы конкурировать с литий-ионными батареями в ЦОДах. Это, например, натрий-ионные батареи на основе электродов, модифицированных берлинской лазурью».

Вместе с тем специалисты-практики проявляют интерес к натрий-ионным технологиям не торопятся. Так, Максим Церулев, технический директор сети дата-центров 3data, подчеркивает: «Говорить о применении Na-ion-батарей в ЦОДах считаю преждевременным. С учетом темпа внедрения существующих технологий в нашей отрасли в перспективе пяти лет более вероятно, что мы будем использовать накопители на суперконденсаторах, чем дождемся внедрения новой катодно-анодной пары».

Следует отметить, что о перспективности суперконденсаторов (т.е. конденсаторов с органическим или неорганическим электролитом, «обкладками» в которых служит двойной электрический слой на границе раздела электрода и электролита; по характеристикам занимают промежуточное положение между конденсаторами и химическими источниками тока) для ЦОДов говорят уже давно, но эта технология никак не «взлетит». С другой стороны, и старые добрые свинцово-кислотные АКБ сбрасывать со счетов не стоит. Они совершенствуются, появляются новые решения для ЦОДов с увеличенным сроком службы. Это проверенные и относительно недорогие решения, что дает им преимущества в бюджетных проектах, где нет специальных требований к компактности и небольшому весу аккумуляторов. Важно, что запасы свинца на планете велики, а процедуры утилизации батарей на его основе хорошо отработаны.

Технологии непрерывно совершенствуются, и, возможно, в не слишком отдаленной перспективе на быстро развивающемся рынке ЦОДов появится новый игрок, который потеснит укрепляющие свои позиции литий-ионные аккумуляторы. ИКС

Вендор в жизни ЦОДа: помощь на всех этапах



Сегодня поставщик комплексных решений для ЦОДов не только поставляет продукцию, но и принимает участие в других стадиях жизненного цикла. Подробнее – Андрей Воробьев, директор центра разработки приложений ЦОД подразделения Secure Power компании Schneider Electric.

– Андрей, давайте начнем с выбора площадки (здания) для ЦОДа. Казалось бы, совсем не вендорская задача. Но особенности площадки/здания могут сильно повлиять на выбор технических решений. Какова роль вендора на этом этапе?

– Существуют два основных варианта работы. Первый – типичный для вендора – сводится к помощи в подборе оборудования. Если заказчик опытный, построил много ЦОДов и постоянно строит новые, то ему этот вариант подойдет. Но если заказчик создает ЦОД первый раз или строит такие объекты нечасто, скажем, раз в три-пять лет, то лучше привлечь специалистов с самого начала проекта. Дело в том, что технологии быстро развиваются, меняются продуктовые линейки, и производитель лучше понимает их специфику.

Особенности площадки могут серьезно повлиять на возможность применения тех или иных технологий. Если заказчик нам доверяет и планирует строить ЦОД с использованием решений Schneider Electric, то имеет смысл обратиться к нашим экспертам, чтобы понять, какие технологии для данной площадки будут оптимальными. Такую работу мы обычно выполняем совместно с другими консультантами.

– Следующий этап – разработка концепции. Насколько он важен?

– Настолько, что ошибки на этом этапе могут серьезно увеличить стоимость и сроки реализации проекта или даже сделать его невыполнимым. Часто концепция разрабатывается одновременно с выбором площадки.

Думаю, еще никому не посчастливилось строить ЦОД в чистом поле с неограниченным количеством ресурсов: электричества, воды и т.п. Всегда с участком связаны те или иные ограничения, которые надо учесть в концепции. Обычно рассматриваются несколько технологических вариантов, в первую очередь для охлаждения машзалов. Был случай, когда «рисовали» 12 концепций. Потом заказчик выбрал одну, которую, кстати, и мы сами предлагали ему как оптимальную для решения его задачи.

При разработке концепции важно, чтобы заказчик четко сформулировал свои технические требования (число стоек, мощность, уровень резервирования и др.) и не менял их впоследствии. Если он вдруг захочет увеличить число стоек или мощность стойки, это может потребовать перехода на другую технологию. И почти всегда приходится искать компромисс. Повысить капитальные затраты, снизив опе-

рационные, или наоборот. Поставить как можно больше стоек с максимальной мощностью или любой ценой вписаться в CAPEX и т.д.

– Возьметесь за разработку концепции, если заказчик не планирует использовать оборудование Schneider Electric?

– Знаете, крайне редко бывает, чтобы в серьезном проекте заказчик исключал использование оборудования Schneider Electric. Как правило, компания входит в шорт-лист основных поставщиков проекта. И наша задача – на этапе концепции доказать, что технологии Schneider Electric будут наилучшими. Если понимаем, что наши продукты в данном случае не будут оптимальными, то честно говорим об этом заказчику.

– Далее – достаточно формализованный этап проектирования. Какие цифровые инструменты могут в этом помочь?

– Наверное, не буду оригинален, если назову BIM. Мы задействуем этот инструмент еще при разработке концепции и продолжаем работать с ним на этапе проектирования. Многие проектировщики используют наши плагины, разработанные для популярных систем BIM. Они позволяют быстро переходить от линейных схем к конкретным спецификациям оборудования, которые подтверждены расчетами. Не надо вручную подбирать модели, они определяются автоматически и помещаются как объекты в 3D-модель.

Мы рекомендуем использовать BIM и на этапе эксплуатации. Но по разным причинам мало кто из заказчиков делает это. В идеале BIM-модель надо применять на всех этапах жизненного цикла ЦОДа. Но цепочка часто рвется, потому что концепцию разрабатывают одни специалисты, проект – другие, строят – третьи, а заказчик непрерывного использования BIM-модели не требует. Хотя появляются заказчики, которые включают это требование в техзадание. Но таких можно пересчитать по пальцам одной руки.

– Рынок стремится строить ЦОДы быстро. Однако пандемия усложнила логистику, многие заказчики жалуются на существенные задержки с поставкой оборудования. Что предприняла Schneider Electric, чтобы решить эту проблему?

– Есть несколько моментов. Первый – прогнозирование. Если к нам приходят в последний момент и просят быстро привезти мегаваттные чиллеры, то могут возникнуть определенные сложности. Мы находимся в глобальной цепочке поставок. Проблема может быть даже не в том, что наш завод не успеет собрать такой чиллер, а в том, что какой-нибудь теплообменник для него не будет поставлен на завод вовремя. Мы можем брать на себя риски и заказывать оборудование заранее, но тогда должны быть вовлечены в проект и понимать ситуацию. Упрощает задачу использование заказчиком стандартных решений. Если он строит ЦОД очередями и устанавливает одни и те же модели, то проще спланировать их производство и поставку.

Второе – мы рекомендуем избегать использования заказных решений. Это так называемые решения ЕТО (Engineered-To-Order), которые требуется специально разработать или доработать. Подобных решений на складах точно не держат. Об этом на этапе концепции тоже надо помнить. Например, мы многим заказчикам советуем в концепцию закладывать менее мощные системы, скажем, с двухмегаваттных систем переходить на машины по 0,5 МВт. Это уже массовые продукты, которые будут поставлены гораздо быстрее.

И третье – локализация. Мы стараемся производить в России продукты, которые часто приходится адаптировать к конкретным проектам, например, различные байпасные шкафы, шкафы ввода-вывода и шкафы распределения, стеллажи для батарей и т.д. Локальная сборка таких решений позволяет более оперативно доставлять их заказчикам.

– Итак, оборудование поставлено, ЦОД построен, что дальше?

– Дальше очень важный этап – приемосдаточные испытания ЦОДа. Причем он важен именно для заказчика. Для тех, кто строит ЦОД, идеальный вариант может выглядеть так: оборудование включили, лампочки зеленые горят, все работает, отлично... Задача заказчика – проверить все на полной нагрузке и во всех режимах. Если что-либо пропустить, проблемы могут начаться при увеличении нагрузки в действующем ЦОДе. Мы помогаем заказчику разрабатывать методику таких испытаний. И проводить их, если у него нет своих компетенций.

– Переходим к самому длительному этапу, эксплуатации. Чем вендор может помочь на этом этапе?

– Важно создать процедуры эксплуатации, чтобы минимизировать негативное влияние человеческого фактора и обеспечить бесперебойную работу ЦОДа. Мы помогаем разработать эти процедуры и внедрить их.

Также важно правильно обслуживать оборудование. Допустим, производитель рекомендует выполнять какую-нибудь операцию каждые полгода. Но оборудование эксплуатируется в разных условиях, поэтому где-то это надо будет делать каждый квартал, а где-то можно и раз в год. Современные технологии позволяют отслеживать текущее состояние оборудования и в зависимости от этого состояния планировать техобслуживание.

Предиктивное реагирование обеспечивают и наши сервисы, использующие результаты анализа работы оборудования на многих площадках по всему миру. Изучение статистики отказов позволяет выработать рекомендации для конкретного устройства, чтобы не допустить деградации его характеристик или выхода из строя.

– А что Schneider Electric предлагает для модернизации ЦОДов? Как удается повысить их эффективность?

– Не хочу вас разочаровывать, но желание заказчика повысить энергоэффективность редко является причиной модернизации. К тому же требования эффективности практически всегда требуют поиска компромисса с отказоустойчивостью. Заказчику же гораздо важнее на 200% гарантировать бесперебойность работы, чем повысить эффективность, даже если экономия может достигать 10–20% совокупных затрат.

Одна из основных причин модернизации – изменение тех или иных требований: увеличить число стоек, мощность на стойку, повысить уровень резервирования и т.п. Другая причина – системные сбои, когда что-нибудь перегревается и отключается. Возможно, ЦОД не был протестирован при полной нагрузке. Когда нагрузка была невелика, все работало нормально, нагрузка увеличилась – начались проблемы. Наконец, третья причина – выход из строя отдельных компонентов.

В зависимости от того, какую задачу надо решить, мы по-разному подходим к модернизации ЦОДа. В качестве примера приведу наш сервис обновления оборудования (retrofit). Допустим, у заказчика стоят модульные ИБП, и силовые модули уже износились. Возникает риск, что они начнут выходить из строя. Мы подбираем подходящие модули (возможно, что точно такие же уже не производятся) и заменяем «начинку» шкафа ИБП, увеличивая срок службы всего изделия. Делается это быстро, не нужно ничего заново согласовывать, перекоммутировать.

– Наконец, финальный этап – утилизация оборудования. Знаю, что некоторые заказчики уже волнуются по поводу утилизации литий-ионных АКБ, а соответствующие процедуры еще не выработаны. Что вы можете ответить таким заказчиком?

– Думаю, опасения напрасны. ЦОДы не пионеры в области применения ЛИ АКБ. Электротранспорт использует такие аккумуляторы уже лет пять, еще дольше они служат в мобильных устройствах. Вопрос утилизации не специфичен для ЦОДов. Кроме того, в России, в частности на Урале, уже есть мощности по переработке ЛИ АКБ. Они готовы брать такие аккумуляторы на утилизацию. И мы, конечно, всегда готовы помочь заказчикам с утилизацией оборудования, равно как и на всех других этапах жизненного цикла ЦОДа.

Гениальность или абсурд? О способах снижения энергопотребления



Александра Эрлих,
генеральный директор,
Анна Галкина (Васильева),
руководитель консультационного центра,
«ПрофАйТи-Кул»

Система охлаждения – одна из самых больших статей расходов любого ЦОДа. Какая же технология охлаждения наиболее эффективна с экономической точки зрения?

Известный немецкий журналист и автор книг Франц Альт однажды сказал: «Самая тяжелая и важная война 21-го столетия будет вестись без оружия. Инструментами этой войны станут энергоэффективность, экономия энергии и ее альтернативные источники». Как в любой войне, в этой больше политики, чем логики. Но, задумавшись о том, сколько энергии потребляют центры обработки данных, понимаешь, что мы находимся на одном из самых горячих фронтов. И, как в любой войне, выиграет тот, чьи инструменты будут более эффективными.

В рамках этой статьи мы проанализируем несколько альтернативных способов охлаждения ЦОДов с целью определить, насколько они на самом деле эффективны – не только с точки зрения экономии ресурсов, но и с точки зрения экономической.

Тепловые насосы

Тепловые насосы давно утвердились в частном секторе. Естественно, что на них обратили внимание инженеры из различных отраслей промышленности и в частности из индустрии ЦОДов.

Безусловно, этот способ получения холода летом и тепла зимой эффективен в тех странах, где, с одной стороны, разрешено использование грунтовых вод в такого рода целях, а с другой –

применяются драконовские экономические меры, направленные на уменьшение выбросов CO₂ (т.е. потребления природного газа и угля) в атмосферу. Попробуем проанализировать, насколько эффективными могут быть тепловые насосы в России.

По способу забора низкопотенциального тепла тепловые насосы принято делить на следующие категории:

- геотермальные;
- воздушные;
- рекуперативные (с утилизацией тепла).

Помимо энергоэффективности системы для применения в ЦОДах не менее важна ее надежность. В свою очередь, надежность получения энергии посредством теплового насоса напрямую зависит от стабильности источника тепла, не подверженного значительным изменениям в течение года. С этой точки зрения системы, включающие в себя воздушные тепловые насосы, можно из рассмотрения исключить.

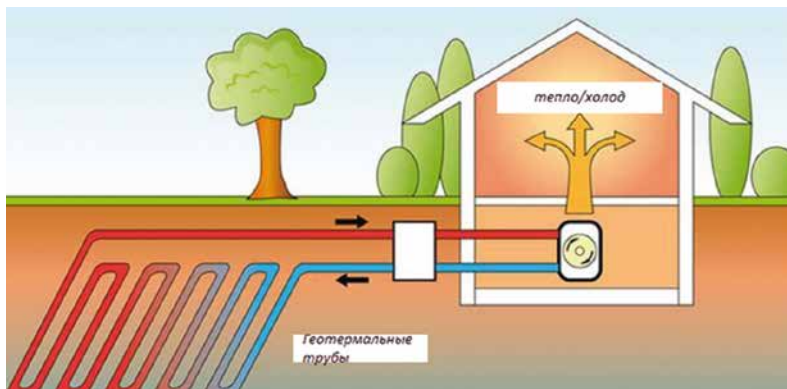
Итак, остаются два вида тепловых насосов: геотермальные и рекуперативные.

Геотермальные насосы

Поскольку использование грунтовых вод в России запрещено, рассмотрим геотермальные тепловые насосы (рис. 1).

Для стабильной работы такого насоса с целью избежать влияния промерзания почвы трубки должны располагаться на значительной глубине (в Москве, например, более 10 м). Стоимость 1 м такой трубы по самым оптимистичным расчетам составляет 10 евро. Теплосъем с одного погонного метра сильно зависит от грунта, в котором располагаются тепловые трубки, но можно сделать грубую оценку себестоимости. Для охлаждения ЦОДа с ИТ-нагрузкой около 200 МВт потребуется участок площадью примерно 6 тыс. кв. м (в случае применения горизонтальных зондов) либо около 30 верти-

Рис. 1. Работа геотермального теплового насоса в жилом доме ▼



кальных скважин с расстоянием минимум 1 м между ними. Даже если у вас достаточно площади, чтобы разместить вокруг ЦОДа такого рода систему, себестоимость самого насоса при этом составит порядка 1–1,2 млн евро. При текущей стоимости электроэнергии в России система просто не сможет окупиться в течение срока эксплуатации.

Тепловые насосы-рекуператоры

Охлаждая ЦОД традиционной системой с чиллером или выносными конденсаторами/драйкулерами, мы сбрасываем избыточное тепло в атмосферу. Жалко, неэкологично, да и проблема с размещением наружных блоков, предназначенных для такого сброса, возникает, наверное, на каждом втором объекте. Неудивительно, что идея полезного использования избыточного тепла ЦОДа постоянно будоражит наш рынок. На первый взгляд, ЦОД отвечает всем требованиям эффективности такого рода тепловых насосов:

- имеется постоянный источник тепла;
- можно рассчитать систему таким образом, чтобы разница температур между источником и потребителем тепла попала в нужный диапазон;
- российский рынок ЦОДов обладает достаточным количеством специалистов, способных грамотно рассчитать систему.

Не хватает лишь одного, но, к сожалению, самого важного фактора: постоянного потребителя тепла. Использование избыточного тепла в качестве источника отопления здания ограничено зимним периодом, а летом снова придется выбрасывать тепло в атмосферу. Получение горячей воды теоретически возможно круглогодично, но в России температура холодной воды (в системе холодоснабжения) значительно колеблется в течение года, и необходимую разницу температур между источником и потребителем тепла невозможно выдерживать постоянно. При детальном рассмотрении любой из систем, удачно эксплуатирующихся в странах Средиземноморья, понимаешь, что в условиях российского климата они не обеспечат надежного отвода избыточного тепла круглый год и потребуют параллельной резервной системы охлаждения.

Помимо физических факторов, препятствующих применению рекуперации в дата-центрах, есть и экономические. Даже в Германии, где стоимость 1 кВт электроэнергии значительно выше, чем в России, и существуют дополнительные расходы – 25 евро за каждую тонну выброшенного в атмосферу CO_2 , окупаемость такого рода систем на сегодняшний день составляет 10 лет. В РФ такая система не окупится никогда.

Тепловые трубы

Теплообмен в тепловой трубке основан на капиллярном эффекте и фазовом переходе теплоносителя из одного агрегатного состояния в другое. Сама технология крайне заманчива, так как в ней используется один из самых энергоемких процессов – фазовый переход. Сопоставим цифры, например, для воды: для ее охлаждения или нагрева на 1°C требуется 4,2 кДж/кг энергии, а для испарения или конденсации – 2258 кДж/кг, т.е. почти в 538 раз больше. Не вдаваясь в подробности, скажем, что возможность «приручить» процесс фазового перехода, а в идеале еще и без повышения давления — это значительное сжатие аппаратного комплекса системы (причем все равно – нагрева или охлаждения) с точки зрения металлоемкости и, как следствие, – снижение капитальных затрат. Понятно, почему эта технология нашла широкое применение как в бытовой технике (в 1966 г. была выпущена первая кухонная плита на основе тепловых трубок), так и в космической отрасли.

Тепловая трубка, или термосифон, может быть прекрасным решением для охлаждения ИТ-оборудования при отсутствии площади для полноценной системы охлаждения. К сожалению, сегодня в ИТ-сфере технология реализуется локально: тепловая трубка на воде или фреоне монтируется непосредственно в конструкцию сервера (рис. 2). С точки зрения теплообмена все замечательно, так как потери минимальны. Но с практической точки зрения картина иная: при использовании данной технологии остро стоит вопрос распределения гарантийных обязательств. Редкий производитель серверного оборудования согласится сохранить гарантию на свою продукцию при нарушении целостности его конструкций, не говоря уже об опасной близости с водой (в случае тепловой трубки на воде). Возможно, поэтому тепловые трубы пока не нашли достаточно широкого применения.



◀ Рис. 2.
Компьютерная
тепловая трубка

А что, если применить термосифонную технологию, не пытаясь завести тепловую трубку в сервер? Скажем, прецизионный кондиционер на фреоне и без компрессора? Такое решение определенно имело бы более широкое распространение и, наверное, за ним будущее.

Иммерсионное охлаждение

Мы все знаем: для того чтобы передавать тепло, необходимы частицы. Поэтому теплопроводность вакуума нулевая, у газов чуть выше (например, у воздуха – 0,022 Вт/м·К), у жидкостей еще выше (так, у трансформаторного масла – 0,11 Вт/м·К, у воды – 0,56 Вт/м·К), а у твердых веществ выше на порядки... Очевидно, что охлаждение жидким веществом с большей теплопроводностью намного эффективнее, чем воздухом. Поэтому появилась идея прямого охлаждения ИТ-оборудования жидкостью более теплопроводной, чем воздух. В идеале хорошо бы попробовать охлаждать серверы жидкостью напрямую, но есть нюанс: эта жидкость должна быть диэлектриком. Конечно, есть на рынке действительно диэлектрические жидкости, но тут прослеживается следующая закономерность: чем более ярко выражены диэлектрические свойства жидкости, тем она менее теплопроводна. Кроме того, диэлектрические жидкости достаточно дороги, а для охлаждения ИТ-оборудования требуются немалые циркуляционные объемы.

Так топить ИТ-оборудование или нет? Скорее нет, чем да. С точки зрения теплообмена решение эффективно, но на практике, как и в случае с тепловыми трубками, сталкиваемся с трудностями сохранения гарантии на серверное оборудование. Чтобы перенастроить или проверить правильность работы/подключения ИТ-оборудования в подобной системе, необходимо извлечь его из охлаждающей емкости, просушить и только после этого выполнять с ним какие-либо действия. Работать с такой системой крайне долго и трудоемко, как для специалистов, осуществляющих эксплуатацию системы охлаждения, так и для ИТ-специалистов.

Системы прямого фрикулинга

Принцип прост: мы уходим от компрессорно-го охлаждения и используем в качестве источника холода воздух. К преимуществам систем прямого фрикулинга небезосновательно относятся низкие капитальные затраты и малое энергопотребление.

Такого рода системы довольно давно известны в мире ЦОДов. В Европе есть несколько инсталляций, да и в России работают две компании, выбравшие именно этот способ охлаждения машзала в качестве основного. Почему же прямой фрикулинг не получил повсеместного распространения? Рассмотрим несколько примеров.

ЦОДы известной российской транснациональной ИТ-компании

Безусловно революционно и провокативно. Никакой компрессорной системы, полное от-

сутствие теплообменников в системе охлаждения. Исключительно воздуховоды и вентиляторы. Однозначно самые низкие на сегодня инвестиционные и энергетические затраты. Но применение такого вида охлаждения в большинстве ЦОДов невозможно по двум веским причинам.

1. **Температуры.** Невозможно подать в холодный коридор воздух с температурой ниже, чем температура охлаждающей среды плюс потери на преодоление сопротивления теплообмену. Поскольку охлаждающей средой в такой версии прямого фрикулинга является окружающий воздух, легко можно вычислить температуру в холодном коридоре летом. И она, к сожалению, весьма далека от требуемых рынком +22–24°C. Недавно довелось дискутировать с представителями компании об эффективности их системы. Полностью с ними согласна: лет через пятьдесят +40–50°C на процессоре станут нормой. Но мы строим ЦОДы сегодня.

2. **Влажность.** В системах прямого фрикулинга контроль и соблюдение коридора влажности, рекомендуемого производителями ИТ-оборудования, не предусматриваются. И все бы ничего, если бы это были лишь требования производителей. Так, для многих корпоративных ЦОДов, применяющих стойки собственной разработки, фактор влажности, казалось бы, теряет свое значение. Однако в спорах о влажности большинство оппонентов забывают о том, что при высокой влажности в ЦОДе резко возрастает потребление самого ИТ-оборудования, стремящегося самостоятельно регулировать конденсацию. А тут уже под угрозой одно из основных преимуществ прямого фрикулинга – низкие энергозатраты.

ЦОД российской технологической компании, предоставляющей облачные инфраструктурные сервисы и услуги дата-центров

Владельцев ЦОДа привлекло второе существенное преимущество систем (не)прямого фрикулинга, а именно низкие капзатраты. Они задались целью использовать эти системы и все-таки добиться в машзале температуры +24°C. А почему бы и нет?

В Москве, например, температура ниже +24°C держится в среднем около 93% времени – 11 месяцев в году. Для обеспечения микроклимата в ЦОДе в оставшиеся 7% времени, когда температура выше +24°C, нужно либо доукомплектовать систему дополнительным охлаждением, либо поднимать температуру в машинном зале, если позволяет ИТ-оборудование.

Найденное решение предусматривало, с одной стороны, испарение воды в качестве дополнительного охлаждения, а именно применение

адиабатики с использованием матов, а с другой – кратковременное поднятие температуры в машинном зале до +28°C.

Но тут снова мечты о дешевом холоде разбились о физические и экономические законы.

Толщина мата, применяемого в этом виде адиабатики, должна быть достаточной для того, чтобы процесс испарения при заданной скорости воздуха успел совершиться – примерно 300 мм. При этом сопротивление по воздуху на чистом мате такой толщины составляет около 200 Па. В процессе испарения мат стремительно загрязняется, соты, предназначенные для прохождения воздуха, и без того мелкие, становятся еще мельче, и сопротивление по воздуху растет в геометрической прогрессии. А вместе с ним и потребление вентиляторов. В связи с этим неприятным эффектом маты приходится менять довольно часто, и тут уже страдает экономика, поскольку относительно низкий CAPEX выливается в очень высокий OPEX.

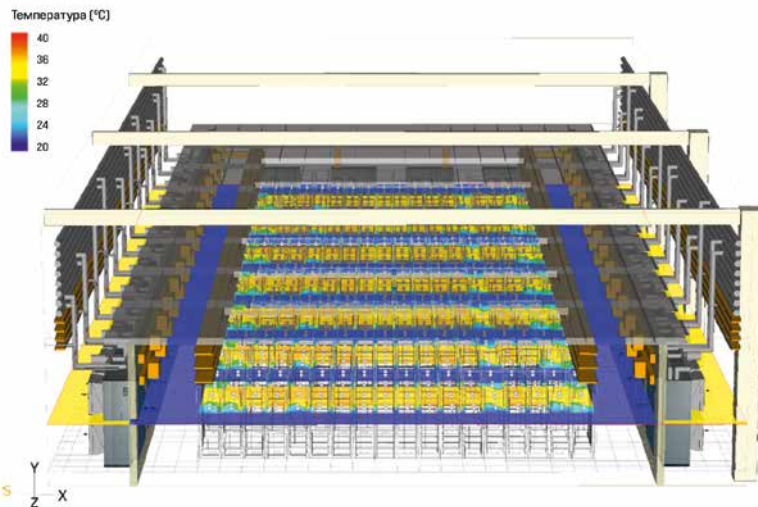
Кроме того, как оказалось, ненужность водоподготовки при применении такой системы – всего лишь рекламный миф. Водоподготовка необходима не только для того, чтобы маты засорялись не слишком быстро, но и для того, чтобы систему воздухопроводов не пришлось менять после первого же года эксплуатации. С учетом системы водоподготовки перестает быть низким не только OPEX, но и CAPEX.

Если говорить о температурных режимах, то поддержание максимальной температуры в машзале даже +28°C в системе этого ЦОДа весьма спорно. Поскольку летом в Москве температура на улице может подниматься выше +32°C, влажность воздуха при этом высока, и в системе предусмотрен рекуператор, обладающий собственным термическим сопротивлением.

ЦОД Centron в Бамберге (земля Бавария, Германия)

Выбранная для этого ЦОДа вентиляционная прямоточная система обеспечивает 95% времени года бескомпрессорную работу при сохранении температуры в машзале не выше +24°C. По очень простой причине: максимальная температура воздуха в этом городе составляет 25,7°C, и наблюдается она всего лишь несколько часов в одном месяце года, в июле. Остальное время года температура воздуха в Бамберге с всего лишь 3,7 солнечных часов в месяце колеблется в интервале от -2,5 до +24°C при среднегодовой температуре +14,4°C. Вторая особенность местного климата – повышенная влажность воздуха

*См., например, Эрлих А., Галкина А., Казаков В. Битва за монополию, или Прецизионные кондиционеры vs. воздухоохлаждающие приборы. «ИКС» № 2'2021, с. 52.



ха. Поэтому, не мудрствуя лукаво, на оставшиеся 5% времени в году в системе просто предусмотрели компрессорное охлаждение.

Низкоскоростное распределение воздуха – Low Speed Ventilation

Не секрет, что мы усиленно пропагандируем применение воздухоохлаждающих приборов (ВОПов) в системах, основанных на принципе низкоскоростного распределения воздуха. Более подробно о ВОПах можно прочесть в других наших статьях* и в наших презентациях. Сейчас затронем лишь основные аспекты.

Если бы мы заговорили об этой системе на заре прихода в ЦОДы прецизионных кондиционеров, а именно на рубеже 60–70-х гг. прошлого века, то услышали бы в ответ: «Да, наверное, когда-нибудь в будущем». Но сегодня, когда температуры в машинном зале +22–24°C стали нормой, это будущее уже наступило.

Правильно спроектированная система низкоскоростного распределения воздуха на базе ВОПа (рис. 4) позволяет экономить порядка 60% электроэнергии по сравнению с привычными системами охлаждения за счет таких факторов, как высокая доля фрикулинга (например, в Москве это 80–85% времени в году), низкое потребление вентиляторов, насосов и пр.

Применение такой системы делает ненужными сразу несколько вспомогательных систем, в частности систему увлажнения и фальшпол. За счет экономии электроэнергии существенно снижаются затраты на систему энергоснабжения. CAPEX ее соизмерим с затратами на систему непрямого фрикулинга с применением адиабатики. А вот эксплуатация значительно проще. Единственное, что сдерживает распространение этих систем в России – малая известность. Но и этот фактор легко преодолим. ИКС

▲ Рис. 4. Распределение температуры в машинном зале при низкоскоростном распределении воздуха

ЦОД для банка: надежность и масштабируемость

Дата-центр, созданный компанией «Инфосистемы Джет» для банка «Открытие», позволил повысить надежность ИТ-инфраструктуры, оптимизировать затраты на ее эксплуатацию и обеспечил возможность быстрого наращивания вычислительной мощности в будущем.

В конце июля 2021 г. банк «Открытие» объявил о вводе в эксплуатацию центра обработки данных для компаний финансовой группы «Открытие». Технологическим партнером банка в этом проекте выступила компания «Инфосистемы Джет».

Предпосылки и подготовка к строительству

До создания основного ЦОДа семь крупных организаций, входящих в финансовую группу «Открытие», эксплуатировали более 500 стоек на 24 собственных и пяти арендованных серверных площадках. Такую распределенную структуру было трудно поддерживать и развивать. Кроме того, серверные были реализованы на недостаточно высоком технологическом уровне и не могли обеспечить требуемую надежность. Инженерное и ИТ-оборудование было разнородным, и каждую площадку обслуживала своя команда эксплуатации. Усложняло работу большое количество арендодателей и поставщиков услуг.

Для поиска путей решения проблем банк привлек ИТ-компанию «Инфосистемы Джет». Совместно со специалистами банка эксперты компании оценили ТСО при различных подходах и пришли к выводу, что оптимальный вариант – построение централизованной архитектуры финансовой группы на базе собственного основного дата-центра и аренды площадей в коммерческом в качестве резерва.

Проектирование и выбор вендоров

Выбор площадки занял несколько месяцев. Остановились на варианте браунфилд (создание ЦОДа в существующем здании). Подробно, с выполнением эскизных проектов, рассмотрели несколько зданий, изучили особенности конструкции каждого из них и вынесли заключения о пригодности и затратах на адаптацию. В итоге выбрали здание советской постройки в районе ул. Окская недалеко от МКАД. Одно из важных преимуществ площадки – возможность подведения дополнительной электрической мощности.

Банк провел проектно-изыскательские работы и представил отчеты, которые специалисты «Инфосистемы Джет» дополнили в отдельных точках. В частности, выяснилось, что при строительстве были использованы ригели (опорные балки) не одного типа, а трех, причем два из них – с меньшим сечением арматуры. Такие места были дополнительно обследованы и усилены. Были также усилены несущие колонны и фундамент.

Для каждой инженерной подсистемы был выбран оптимальный вендор: для ИБП – Vertiv, для дизель-генераторов – SDMO, для чиллерных установок и кондиционеров – Stulz. Поставку продукции Stulz осуществила компания HTS, официальный дистрибьютор Stulz на территории России. Компания Schneider Electric для этого проекта разработала независимую систему «парящих» изолированных холодных коридоров: решение Free-Flying позволяет устанавливать серверные стойки различных габаритов в смонтированном коридоре без нарушения целостности системы, по мере необходимости.



Всеволод Воробьев,
руководитель направления ЦОД
центра сетевых решений,
«Инфосистемы Джет»

осуществила компания HTS, официальный дистрибьютор Stulz на территории России. Компания Schneider Electric для этого проекта разработала независимую систему «парящих» изолированных холодных коридоров: решение Free-Flying позволяет устанавливать серверные стойки различных габаритов в смонтированном коридоре без нарушения целостности системы, по мере необходимости.

Особенности системы охлаждения

Специалисты HTS предложили классическую схему системы кондиционирования на жидкостном носителе: холодильные машины (чиллеры) Stulz CyberCool 2 наружной установки с фрикулингом и водяные прецизионные кондиционеры Stulz CyberAir 3 PRO с вентиляторной группой, вынесенной под фальшпол. Совокупное энергопотребление этой системы оказалось существенно ниже, чем в предложениях других участников тендера. Причем заявленные производителем характеристики были подтверждены результатами тестирования оборудования на заводе. В результате заказчик смог минимизировать годовое энергопотребление системы холодоснабжения и затраты на электроэнергию, снизив подводимую к объекту электрическую мощность, сократив тем самым капитальные затраты, а также уменьшить стоимость смежных систем ЦОДа.

Чтобы холодильные машины можно было обслуживать с любой стороны и безопасно работать с их верхней частью, в «Инфосистемы Джет» разработали, спроектировали и реализовали специальную раму для установки чиллеров на площадке заказчика.

По словам Алексея Колоколова из компании HTS, для удобства технического обслуживания и проведения регламентных работ вентиляторы на чиллере сделаны откидывающимися, что позволяет в безопасных условиях быстрее и качественнее проводить чистку теплообменников. Кроме того, электрический шкаф чиллера оснащен системой освещения, электрической розеткой и выдвижной крышей, благодаря которой оборудование можно обслуживать вне зависимости от погодных условий в любое время года.

Одно из достоинств выбранного чиллера – встроенный внутренний ИБП, от которого питается контроллер, что обеспечивает непрерывность его работы и быстрый выход на рабочий режим при переключении с одного ввода электро-



питания на другой. Короткое время выхода холодильной машины на рабочий режим (менее 2 мин) дало возможность уменьшить общий объем баков – накопителей жидкости.

Кондиционеры укомплектованы встроенными ИБП для обеспечения непрерывной работы их контроллера и вторым вводом питания, что позволяет не прерывать работу при переключении кондиционера с одного луча питания на другой.

В новом ЦОДе создали два хладоцентра. В первом установлены теплообменники «жидкость – жидкость» между внешним и внутренним контурами. Во втором, находящемся вблизи машзалов, охлажденная в первом хладоцентре вода разводится по кондиционерам шкафного типа. Поскольку кондиционеры расположены в отдельном помещении, специалисты по ИТ не имеют доступа к кондиционерам, а персонал, обслуживающий кондиционеры, не заходит в основной зал. В самих машзалах организована изоляция холодного коридора.

Моделирование, разрешения и строительство

При проектировании основных инженерных систем – энергетических, климатических и слаботочных – компания «Инфосистемы Джет» использовала BIM-технологии, что позволило минимизировать коллизии пересечения кабельных трасс при строительстве. Для того чтобы спрогнозировать распределение воздушных потоков, проводили CFD-моделирование. В частности, изучали воздушные потоки при отключении кондиционера, анализировали, не появляются ли точки перегрева или ненужные завихрения.

Строительство выполнили в рамках капитального ремонта части здания. Это позволило уменьшить количество требуемой разрешительной документации. Заказчик и «Инфосистемы Джет» совместно выполнили комплекс работ по технологическому присоединению к электрическим сетям новой электроустановки мощностью 4 МВт. От момента оформления заявки до подачи напряжения на объект (включая монтаж шести трансформаторных подстанций) прошло всего шесть месяцев.

Компания «Инфосистемы Джет» получала документы на земляные работы, отвечала за организацию техники безопасности на стройплощадке, за пожарную безопасность и охрану периметра объекта. Также компания построила трансформаторную подстанцию на территории заказчика и сдала ее Ростехнадзору.

Проект реализовывался с привлечением проверенных подрядчиков «Инфосистемы Джет». В пиковый момент на

объекте были заняты более 200 человек. Самая активная фаза работы пришлось на весну 2020 г., время самых жестких карантинных ограничений из-за COVID-19. Пришлось дополнительно организовывать контроль температуры сотрудников, изоляцию бригад, получение разрешений на работы. Эти непредвиденные проблемы хоть и затруднили, но не остановили строительство.

Обеспечение надежности и приемо-сдаточные испытания

Электроснабжение в ЦОДе организовали по достаточно редко встречающейся схеме 3/2N. Причем каждый из трех лучей распределения электропитания на всем протяжении трассы от розеток и щитков до ИБП и ДГУ промаркировали своим цветом – черным, желтым и синим.

Схема резервирования системы холодоснабжения следующая: снаружи здания расположен дополнительный чиллер (N + 1), а для охлаждения машзалов установлены по два дополнительных шкафных кондиционера (N + 2). Для каналов связи используется полностью зеркальная схема резервирования 2N.

Сдача проекта проходила в три этапа. Для каждой подсистемы была разработана программа приемо-сдаточных испытаний. Первый этап – индивидуальные испытания каждой подсистемы. Второй – отработка аварийных ситуаций. На этом этапе мы имитировали аварии, например, отключали трансформаторную подстанцию. Для третьего этапа – 72-часового тестирования всех инженерных компонентов при полной проектной нагрузке – арендовали тепловые пушки. В результате и мы, и заказчик убедились, что все системы работают и в штатных, и в нештатных ситуациях, причем при полной нагрузке.

Итоги проекта

От идеи до установки ИТ-оборудования прошло почти три года. На территории площадью около 1 га построен дата-центр емкостью 366 стоек с общим энергопотреблением 4 МВт. Серверные стойки размещаются в трех из четырех существующих независимых машинных залов. В настоящее время установлены 192 стойки – в основном с потреблением 7 кВт, но есть и высоконагруженные – 14 кВт.

Помимо машзала и инженерных помещений создано более десятка вспомогательных помещений – кабинеты, переговорные, санузлы и кухня. Развернуты специальные склады для временного хранения оборудования и склад ЗИП.

Во все инженерные решения заложена возможность быстрого масштабирования. На несколько лет заказчик будет полностью обеспечен вычислительными мощностями. И самое главное – проведена централизация ИТ-инфраструктуры, что позволяет оптимизировать затраты на эксплуатацию и повысить доступность ИТ-сервисов.

Проект оказался самым крупным по направлению цодо-строения в 30-летней истории компании «Инфосистемы Джет».

Автоматизация ЦОДа: шесть аспектов проектирования и эксплуатации



Илья Савинкин, инженер-эксперт департамента инженерных и мультимедийных систем, КРОК

В дата-центре присутствуют практически все инженерные системы – вентиляции, кондиционирования, холодоснабжения и теплоснабжения, энергоснабжения и освещения. Каковы особенности автоматизации этих систем?

Систему автоматизации ЦОДа можно условно разделить на три уровня: нижний (полевой) – датчики и исполнительные устройства; средний – контроллеры; верхний – ПО и центральный сервер.

Локальная автоматизация и ее отказоустойчивость

Средства автоматизации должны отвечать всем требованиям, предъявляемым к надежности ЦОДа в целом. Если объект предполагается сертифицировать согласно уровням Tier, то и автоматика должна иметь соответствующий уровень отказоустойчивости.

На нижнем уровне для автоматизации процессов работы ЦОДа, как правило, выбираются надежные, доказавшие свою эффективность решения: промышленные и полупромышленные варианты исполнения датчиков, провод-

ные линии связи, резервированные схемы управления. Также обязательно предусматриваются аварийные ручные режимы.

Чтобы обеспечить непрерывность работы ЦОДа и возможность обслуживания оборудования без остановки работы комплекса, все средства автоматизации должны быть резервированы в той же степени, что и само оборудование. Например, два резервированных насоса для прокачки хладагента, запитанные по двум независимым веткам первой категории надежности, но управляемые одним контроллером автоматизации, не обеспечат безостановочной работы в случае отказа этого контроллера. Отключение или выход из строя любого щита локальной автоматики не должны сказываться на работе соседних резервных агрегатов. Кроме того, логика работы оборудования должна сохраняться.

Критически важно, чтобы на этапе разработки проекта проектировщики смежных систем взаимодействовали между собой и надежность одних систем не страдала от экономии на других. При запуске ЦОДа в эксплуатацию необходимо промоделировать аварийные ситуации для оценки функционирования всех систем в комплексе.



Обмен данными

В большинстве случаев данные от контроллеров передаются в центральный сервер по сети Ethernet. В зависимости от размеров ЦОДа используют либо собственные коммутаторы сети, либо выделенный сегмент СКС с резервированным кольцом для передачи данных. Изолированная технологическая сеть позволяет избежать конфликтов с политиками безопасности и нюансами настройки сетевых взаимодействий. Важны постоянная доступность сети и минимальное вмешательство в ее настройки в период всей эксплуатации.

В отдельных случаях оправдывают себя шинные протоколы передачи данных – для передачи некритичных данных с большого количества устройств, например, с измерителей параметров энергопотребления для каждой стойки в коммерческих ЦОДах.

При разработке систем контроля крупных дата-центров мы рекомендуем отталкиваться не только от топовых решений, но и от потребностей заказчика и характера использования ЦОДа. Так, если нужно измерять энергопотребление и контролировать напряжение на каждой стойке, то далеко не всегда оправданно подключать все распределители питания (PDU) напрямую к ЛВС. Целесообразнее установить боксы с самыми простыми электросчетчиками на отводящих линиях к стойкам или применять токовые трансформаторы с общим контроллером.



Верхний уровень и резервирование

При высоких требованиях к отказоустойчивости обязательно резервируется центральный сервер, дублируются питание и жесткие диски для хранения данных (в случае физического сервера). Один из вариантов повышения отказоустойчивости – виртуализация сервера.

С точки зрения ПО автоматизации основное отличие дата-центров от административных зданий – детализация технологических процессов для диспетчера и архивирование всех параметров для дальнейшего анализа и тонкой настройки систем. Детальные архивные данные позволяют анализировать нештатные ситуации с тем, чтобы впоследствии предотвращать их.

К разработке проекта системы автоматизации ЦОДа мы рекомендуем еще на самых ран-

них этапах привлекать службу эксплуатации. Почему? Никто не объяснит требования к интерфейсу и отслеживаемым параметрам точнее и лучше, чем люди, имеющие опыт работы с подобными системами.



Настройка параметров

Отдельно отметим, что автоматизация и контроль энергоснабжения, детальный учет и статистика энергопотребления в ЦОДах находятся на принципиально ином уровне, чем, например, в офисных и административных зданиях. Анализ профилей потребления, контроль качества питания критически важны для стабильной работы всего комплекса. Имея архив со статистическими данными, анализируя взаимосвязи разных событий и параметров, служба эксплуатации может значительно улучшить PUE даже действующего ЦОДа.

В требованиях к системе важно предусмотреть инструментарий для анализа, генерации отчетов и подстройки параметров, влияющих на эффективность систем. Скажем, если температуру перехода системы охлаждения в режим фрикулинга не задавать жестко, а разрешить диспетчеру редактировать, то можно год от года накапливать данные о работе ЦОДа с разной загрузкой и в разных температурных режимах и опытным путем найти наиболее безопасные и энергоэффективные параметры. Система построения графиков и отчеты помогут сравнивать разные режимы в наглядном виде и принимать решения с опорой на статистику.



Моделирование

Тенденция к цифровизации и математическому моделированию не обошла стороной и дата-центры. Сегодня на рынке есть множество предложений для моделирования распределения температур и воздушных потоков в машинных залах. Анализируя показания датчиков, ПО способно выдавать рекомендации по оптимальному перераспределению оборудования с учетом тепловой нагрузки, электропитания и сетевых потребностей.



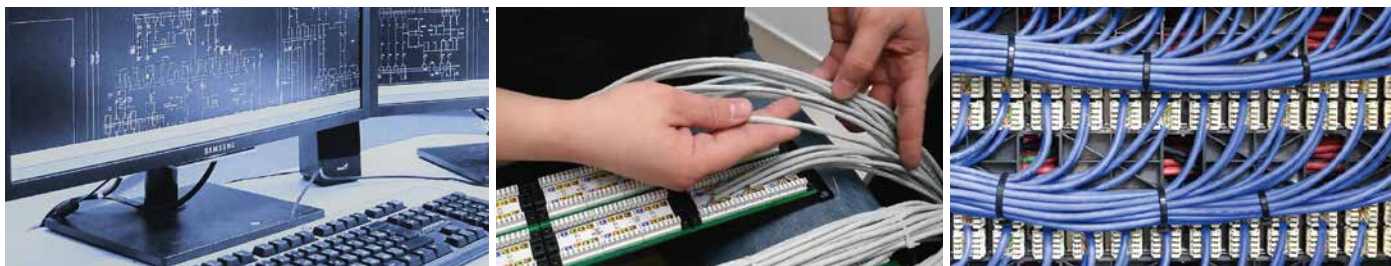
Этапы создания системы автоматизации

Нередко на первом этапе необходимо запустить ЦОД на половину или четверть мощности. Поэтому важно заранее предусмотреть разумное деление систем автоматики. Например, может оказаться менее затратно сразу установить всю автоматику на полный объем и оставить на последующие этапы только автоматику отдельных агрегатов. Однако деление на этапы нужно проводить совместно со специалистами по холдоснабжению, электрике и т.д. **ИКС**

Как и для чего автоматизировать проектирование СКС

Андрей Семенов,
профессор,
МТУСИ

Все СКС для общественных зданий имеют выраженные типовые черты, поэтому естественно автоматизировать их проектирование при помощи специализированных программных средств. Каким может быть такое ПО и в каких областях есть смысл его применять?



Современные общественные здания, даже если они формально не относятся к «умным» домам, оборудуются более или менее развитой системой автоматизации. Она состоит из ряда отдельных подсистем, реализованных по модели открытой архитектуры. При этом нижний физический уровень в большинстве случаев выполняется на основе кабельных каналов связи, а за беспроводными технологиями остаются некоторые нишевые области (например, гостевая сеть Wi-Fi).

Пассивная часть кабельного канала связи формируется на основе структурированной кабельной системы (СКС), которая сегодня де-факто стала таким же обязательным компонентом инженерного обеспечения здания, как водопровод, вентиляция и освещение. Характерная особенность СКС – большое количество пользовательских портов, розетки которых устанавливаются в отдельных помещениях с равномерным распределением по площади.

Любое здание, даже построенное по типовому проекту, уникально в части распределения помещений по владельцам и арендаторам площадей. Как следствие, для него требуется индивидуальное проектирование структурированной проводки, которое выполняется высококвалифицированными специалистами, а это означает рост издержек.

С другой стороны, при всем разнообразии готовых проектов все они демонстрируют явно выраженные типовые черты – хотя бы на том основании, что любая СКС должна отвечать требованиям профильных стандартов (американский TIA/EIA-568С, международный ISO/IEC 11801:2017,

отечественные стандарты групп ГОСТ Р 565xx и ГОСТ Р 582xx). В этой ситуации естественно максимально автоматизировать процесс проектирования при помощи специализированного ПО. Разработка соответствующего пакета программ потенциально привлекательна для софтверных компаний, поскольку СКС массово создаются как в новых, так и в отремонтированных зданиях, что обеспечивает продукту неплохие шансы на коммерческий успех.

Особенности проектирования СКС

Отметим, что как объект проектирования СКС очень неплохо обусловлена: даже при наличии в системе пары сотен портов в ней четко проявляются устойчивые статистические связи, которые «отсекают» подавляющее большинство неоптимальных вариантов. В результате упрощается алгоритмизация, что снижает требования к производительности компьютера, позволяет ускорить получение готового результата и упростить контроль его корректности.

Вычислительные затраты снижаются и за счет немногочисленности ограничений стандартов в части длин стационарных линий и возможных конфигураций панелей коммутационного поля. Кроме того, снижению затрат способствует довольно четкое разделение областей применения классических и MPTL-линий (на уровне рабочих мест и цифрового потолка соответственно) и некоторые иные компонентные и системные особенности СКС.

Особенности элементной базы СКС различных производителей учитываются путем созда-

ния соответствующих библиотек. Благодаря довольно большой схожести продукции по типу исполнения (например, моноблочные и наборные панели, кабели категорий 5e и 6 и т.д.), а также представленной номенклатуры (хороший пример – ряд длин шнуров) библиотека разрабатывается один раз, а чтобы ввести в нее продукцию нового вендора, достаточно модернизировать прототип с переписыванием номеров отдельных компонентов. Последнее означает, что отпускная стоимость соответствующего модуля будет невелика, и потенциально расширяет круг потребителей среди партнеров данного вендора.

Можно ли создать специализированное ПО

СКС даже среднего масштаба с несколькими сотнями портов содержит более тысячи отдельных компонентов и потому представляет собой полноценную техническую систему. Достаточно ограниченная номенклатура этих компонентов позволяет однозначно математически описать такой объект с привлечением формализованных правил и сформировать соответствующую систему уравнений.

Доказать существование решения такой системы не составляет проблемы, поскольку она образована линейными уравнениями, а вот искать само решение «в лоб» в массовой практике проектирования вряд ли целесообразно. Здесь сказывается огромная размерность системы, из чего следует вывод о необходимости привлечь к поиску решения приближенные алгоритмы. При формировании последних можно воспользоваться опытом смежных областей: в качестве прототипа допустимо обратиться, например, к программным продуктам для трассировки печатных плат. Они позволяли получать довольно неплохие результаты еще в середине 80-х гг. прошлого века даже при ограниченных на тот момент вычислительных мощностях компьютеров.

С учетом явно выраженного сходства задач проектирования печатной платы и разработки топологии кабельной системы, а также технического прогресса за четыре десятка лет, для работы программ проектирования СКС – с точки зрения полноты вариантов и времени получе-

ния готового результата – вполне достаточно даже ПК среднего уровня производительности.

Где стоит применять САПР

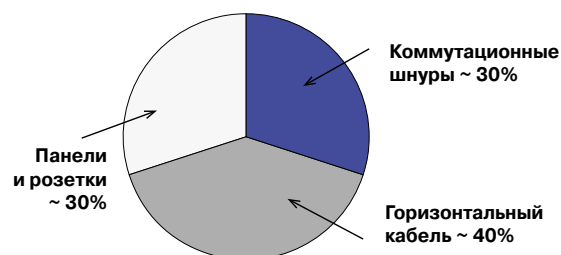
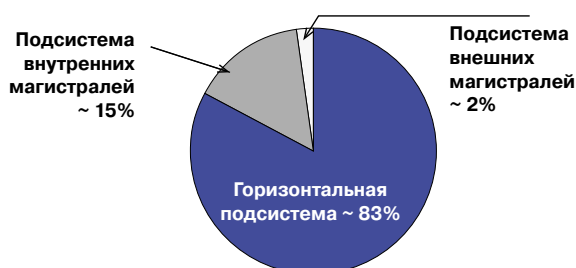
Под специализированным ПО в рассматриваемом контексте понимается САПР. В результате обработки такой программой исходных данных получают:

- графическую часть проекта с указанием мест и особенностей размещения пользовательских розеток и технических помещений, трасс прокладки кабелей, организационно относящихся к горизонтальной и магистральной подсистемам, межэтажных переходов и аналогичных им;
- спецификацию поставляемого оборудования с привязкой к номенклатуре конкретного производителя СКС.

Спецификация дает возможность эффективно проконтролировать качество работы программы за счет упомянутой выше хорошей обусловленности кабельной системы. Для этого пользуются наличием устойчивой связи между расходами на реализацию отдельных подсистем и компонентами для их реализации (рис. 1). Подобный базовый функционал имеется, например, в популярном на отечественном рынке программном продукте «Наноклад-СКС» компании «Нанософт».

Если добавить к этому материалу пояснительную записку, получаем на выходе полноценный технический и/или рабочий проект. Необходимое условие его получения – ввод в программу уникального массива исходных данных, что фактически сводится к расстановке на поэтажных планах здания пользовательских розеток, указанию трасс прокладки лотков, мест расположения стояков и других аналогичных компонентов.

Процедура определения массива исходных данных и их ввода в систему требует довольно много времени и при современном уровне техники не может быть на 100% автоматизирована даже при наличии цифрового двойника здания. Между тем опыт проектов на открытом рынке показывает, что до уровня реализации доводится не более 5% запросов на коммерческое предложение по построению кабельной системы, причем эта доля не зависит от уровня проработки имеющихся исходных данных.



◀ Рис. 1. Статистические связи на системном (слева) и компонентном (справа) уровнях СКС

Такая особенность рынка фактически делает специализированную САПР СКС нишевым продуктом. Использование соответствующего программного комплекса ради оптимизации бизнес-процессов и снижения издержек на операционную деятельность целесообразно только непосредственно в конструкторском бюро. САПР в полной мере демонстрирует свою эффективность исключительно при разработке проектной документации разных уровней по отдельному договору или в рамках комплексного контракта.

Наличие рабочего проекта в виде электронного образа создаваемой структурированной проводки заметно облегчает и формирование исполнительной документации, передаваемой заказчику СКС в составе комплекта документов после завершения монтажа, тестирования и сертификации. Для этого достаточно просто внести изменения в созданные ранее графические файлы. Коррекция спецификации дополнительных затрат не требует, так как выполняется автоматически.

Электронные конфигураторы СКС

Проект построения СКС не ограничивается только созданием проектной документации различного уровня. Если в нем выделить иные составляющие, то возможности использовать преимущества вычислительной техники немедленно расширяются. В основе этого – упомянутая выше хорошая статистическая обусловленность структурированной проводки, что резко сокращает массив безусловно необходимой информации, позволяет получить спецификацию требуемой элементной базы и ее ценовую оценку, а также составить перечень выполняемых работ с оценкой их продолжительности и стоимости.

Необходимые статистические связи задаются в электронной таблице (де-факто Excel), в нее же в соответствующие поля вводятся переменные начальные параметры. Их минимальный список включает:

- категорию кабельной системы и количество портов пользовательской розетки (по умолчанию для выполнения требований стандарта указывается 2);
- количество устанавливаемых пользовательских розеток, указанное прямо или косвенно (через габариты области, обслуживаемой техническим помещением нижнего уровня);
- тип коммутационных панелей и общее количество коммутационных шнуров (с учетом реалий проектов и из соображений экономии в спецификацию шнуров закладывается меньше, чем пользовательских портов);
- высоту этажа и места расположения стояков (при отсутствии стояков в соответствующей ячейке указывается 0);

- выбор типа элементов для формирования кабельных трасс в коридорах и пользовательских помещениях.

Результат работы выдается компьютером немедленно в виде спецификации поставляемого оборудования и перечня производимых работ на отдельном листе.

При необходимости или из соображений расширения функциональных возможностей продукта перечень вводимых данных можно дополнить. Довольно часто встречается, например, расчет системы чистого электропитания (количество розеток на рабочих местах, сечение силовых кабелей, количество и номинал автоматов).

Фактически таблица выполняет функции так называемого конфигуратора, а результат работы используется в качестве основы переменной части коммерческого предложения (эскизного проекта). Необходимое условие получения точной оценки по подобной схеме – типовой характер объекта установки кабельной системы, что на практике выполняется в большинстве случаев.

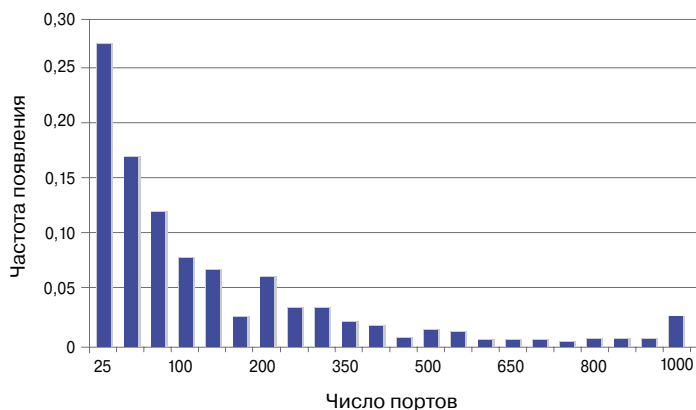
К идее конфигуратора часто приходят сотрудники департаментов продаж системных интеграторов и крупных монтажных организаций, выполняющие заявки продавцов. Его разработка и активное использование в текущей работе – естественная реакция на типовой характер выполняемых действий и стремление к автоматизации рутинной деятельности.

Конфигураторы рассматриваемой разновидности довольно популярны на практике. В большинстве случаев их разрабатывают «под себя», поэтому, как правило, они имеют «слепой» интерфейс (в лучшем случае с выделением соответствующих ячеек цветом, рамкой или текстом), понятный только автору и, возможно, его коллегам по работе.

До уровня продукта массового применения конфигураторы доходят довольно редко. Например, еще в 90-х гг. прошлого века довольно активно рекламировался продукт Net Wizard, который позволял рассчитать комбинированную спецификацию СКС (на базе продуктов Molex) и ЛВС на коммутаторах 3Com.

Иногда конфигураторы доступны через сайты системных интеграторов и монтажных компаний. В этом случае они используются как средство быстрой оценки стоимости проекта без участия менеджера.

Сильная сторона конфигуратора – быстрота получения оценки, которая зачастую формируется в реальном масштабе времени. Это занимает не более 10–15 минут и возможно даже в режиме телефонного разговора. При этом конфигураторы демонстрируют неплохую точность: опытный инженер отдела продаж легко мини-



▲ Рис. 2. Частота реализации информационных кабельных систем с разным числом портов

мизирует расхождение с полноценным проектом до уровня примерно 10%, при условии типового характера объекта.

Графические редакторы СКС

Принципиальный недостаток конфигуратора – отсутствие графической части коммерческого предложения – обусловлен примитивностью встроенного графического редактора Excel, который ориентирован на построение графиков по массиву данных, заданных в табличной форме, а остальные графические образы можно только импортировать. Чтобы преодолеть этот недостаток, были разработаны графические редакторы, дающие возможность включить в коммерческое предложение соответствующий иллюстративный материал.

Немногочисленные фирменные программные продукты работают с встроенной или подключаемой библиотекой компонентов конкретного производителя. Интеллектуальная составляющая работы пользователя сводится к соединению отдельных портов панелей и розеток кабелями. При перемещении панелей и розеток по плоскости чертежа связи не разрываются, что выгодно отличает специализированные редакторы от продуктов общего применения (например, Corel Draw). На основании созданного графического образа кабельной системы легко рассчитывается спецификация поставляемого оборудования и, возможно, составляется перечень выполняемых работ.

Встречаются также продукты этого типа, созданные на базе популярной системы AutoCAD.

Сравнительно невысокая популярность специализированных графических редакторов СКС объясняется слабой востребованностью иллюстративного материала на этапе подготовки и предоставления коммерческого предложения. Это связано с тем, что большинство информационных кабельных систем, во-первых, имеют небольшое количество портов (рис. 2), поскольку



▲ Рис. 3. Иерархия программных продуктов для поддержки проектирования СКС

они развертываются, например, в двух-трех соседних комнатах одного этажа; во-вторых, монтируются в типовых зданиях, что заметно снижает информативность изображения.

Немаловажно также, что предварительная спецификация с помощью графического редактора формируется заметно дольше по сравнению с конфигуратором. Воспользоваться же уже созданными изображениями на этапе технического проекта полноценно не получается из-за того, что перевод работы с потенциальным заказчиком на эту стадию маловероятен.

В результате специализированные графические редакторы занимают в иерархии доступных программных продуктов третье место (рис. 3), хотя по своим функциональным возможностям по меньшей мере не уступают конфигураторам.

◆◆◆

Итак, для проектирования СКС может применяться широкая гамма программных продуктов различного назначения. Для них существует четкое трехуровневое разделение по функциональным возможностям продукта, и в соответствии с этими уровнями они применяются на разных стадиях проекта реализации структурированной информационной проводки.

Фокусная область применения специализированного ПО – проектные организации или отделы инжиниринговых компаний, выпускающие комплекты проектной и рабочей документации. Для сотрудников отдела продаж главным программным инструментом является конфигуратор и в меньшей степени – специализированный графический редактор. Конфигуратор СКС можно создать самостоятельно на базе электронных таблиц Excel.

Производителям СКС имеет смысл предоставлять своим партнерам графическую библиотеку компонентов в нескольких популярных форматах для использования в процессе проектирования. ИКС

EMILINK: производство в России – главное преимущество

Имя EMILINK не очень известно на российском рынке ЦОДов. Однако изготовленные на заводах компании изделия используются на многих ИКТ-объектах. О смещении акцентов на развитие собственных брендов, портфеле продуктов и планах – основатель и руководитель ГК «ЭМИЛИНК» Андрей Зуев.



– Андрей, давайте знакомиться. Пожалуйста, расскажите историю создания и развития компании.

– В середине нулевых быстро развивался рынок оптических систем, операторы связи активно прокладывали оптику, строили сети GPON. Поэтому решил делать оптические патчкорды (коммутационные шнуры. – Прим. ред.). Первое время было очень непросто, вел бизнес на свои деньги, без кредитов и займов, несколько раз появлялись мысли о том, чтобы закрыть дело, но благодаря растущему фантастическими темпами рынку и энтузиазму сотрудников производство постоянно развивалось и крепло. И к 2012 г. компания EMILINK стала крупнейшим производителем патчкордов в России (здесь и далее приводится оценка положения на рынке, сделанная самой EMILINK. – Прим. ред.). Это был первый и самый сложный этап развития моего бизнеса.

– Такой объем продукции (вы говорите о первом месте) просто не может оставаться незамеченным на рынке. Но я патч-кордов вашей марки NTSS на объектах почему-то не видел.

– Вы, скорее всего, никогда не узнаете, что держите в руках именно наш оптический шнур, поскольку чаще всего на нем написано чье-то другое (известное или не очень) имя. Однако примерно каждый третий оптический шнур российского происхождения получил путевку в жизнь на нашем заводе.

– Андрей, в те годы действительно нужна была большая смелость начинать свое производство, а не перепродавать. Но и потом условия проще не становились, и я знаю, что у вас не одно производство.

– На следующем этапе развития – в 2013–2014 гг. – моя компания начала выпускать оптические кроссы. Выбрали площадку, собрали команду смелых и уверенных профессионалов, закупили оборудование. Начинать буквально с нескольких станков, потом станочный парк вырос в пять-шесть раз.

И все получилось. На сегодня мы стали крупнейшим производителем оптических кроссов в России. Снабжаем ими всех крупных продавцов, которые поставляют их в том числе под своими брендами.



История с OEM-заказами, как и в случае с патчкордами, повторилась и с подразделением металлообработки.

– Оптические шнуры, кроссы, что дальше?

– Как выяснилось, шнуры и кроссы – это только начало приключений для производителей. Мы перешли к изготовлению более сложных изделий: телекоммуникационных и сетевых шкафов, шкафов для центров обработки данных. Освоили производство систем изоляции холодных (горячих) коридоров для ЦОДов. И в настоящее время мы выпускаем широчайший ассортимент продукции из листового металла и алюминия для ИКТ-отрасли.

– Насколько знаю, вы занимаетесь еще и производством оптического кабеля?

– Да, на заводе «КОСТРОМАКАБЕЛЬ». Как и все наши основные производственные площадки, он находится в Костроме. На заводе нами освоен выпуск всех основных типов волоконно-оптического кабеля, в том числе для ЦОДов.

Мы идем по пути максимальной замены сырья и комплектующих в ассортименте продукции на элементы собственного производства. Начали делать патчкорды, для них стали производить свои оптические кроссы, свой кабель и т.д.

– Но, как вы уже упоминали, большую долю продукции вы производите по OEM-контрактам, и она поставляется на рынок под другими брендами.

– Да, это так. Например, в сегменте решений для ЦОДов по OEM-контрактам мы выпускаем около 70% продукции. В сегменте телеком-решений – примерно половину. Но в России работать по OEM-модели – дело благодарное. Хотим поставлять больше продукции под своими брендами.

– Если говорить о кабельных решениях для ЦОДов, где важны высокая плотность и производительность, то насколько здесь отечественные продукты конкурентоспособны?

– Считаю, что мы производим самые современные решения, отвечающие всем требованиям ЦОДов. В сегменте медножильных СКС под брендом NTSS предлагаем системы самых высоких категорий – все с системной гарантией. Но инфраструктура ЦОДов – это главным образом оптика. Используем оптическое волокно разных производителей – как

отечественных (одномодовое волокно АО «Оптическое волоконные системы» из Саранска), так и зарубежных (многосовое волокно классов OM3, OM4 и OM5 одного из мировых лидеров компании Corning). Основную ставку делаем на претерминированные решения с многосовыми (групповыми) разъемами MPO/MTP – то, что наиболее востребовано в ЦОДах. Качественно изготавливаем кабель, шнуры, сборки, причем готовы оперативно подстраиваться под требования конкретного проекта – обеспечивать нужные длины кабельных сборок и т.д.

– Возможность оперативно кастомизировать решения в соответствии с требованиями конкретного проекта – это, наверное, одно из основных преимуществ собственного производства?

– Да, кастомизация – наше важное преимущество. Мы можем быстро изготовить на заказ любые оптические решения, в том числе высокой плотности. За несколько недель разрабатываем и выпускаем на своих заводах решения по техническому заданию заказчика, учитывая все его специфические пожелания. То же самое относится и к металлическим конструкциям: готовы оперативно внести любые изменения, например, сделать дополнительные отверстия для ввода кабелей, специальные системы притока-оттока воздуха, адаптировать решение к специальным условиям эксплуатации и т.п.

Кроме того, свое производство – это максимальный контроль качества и возможность предложить лучшие цены. Уверен, что и среди серверных шкафов наше предложение – наилучшее по соотношению «цена – качество».

– Расскажите подробнее, какие шкафные решения вы предлагаете ЦОДам.

– Для ЦОДов мы разработали и производим три линейки специализированных шкафов. Наши «тяжеловесы» – серия ПРОЦОД, куда входят как сварные (несущая способность 2 т), так и разборные (1,8 т) шкафы. Новая, облегченная серия DS – более гибкая в применении (продукты этой серии можно использовать не только как серверные, но и как шкафы высокой нагрузки для АКБ, ИБП и кроссовые шкафы). Функционал шкафов серии DS быстро расширяется. Наконец, серия Colocation с отдельным доступом в шкаф оптимизирована для коммерческих ЦОДов. В прошлом году мы поставили на рынок около 2 тыс. серверных шкафов.

Как я уже упоминал, для ЦОДов мы производим и систему изоляции коридоров. Сейчас находимся в стадии перехода от системы первого поколения к новому, модульному решению, которое обеспечит свободное размещение шкафов любых размеров.

– Ряд российских производителей стараются дополнять свои конструктивы другими инженерными системами. Какова ваша позиция?

– Мы не ощущаем, чтобы заказчики повсеместно требовали комплексные решения от одного производителя. Относительно предложения блоков охлаждения пока анализируем ситуацию. Заказчики часто сами решают задачи охлаждения, покупая только металлические конструкции.

Еще раз подчеркну нашу позицию: мы стремимся предлагать рынку то, что производим сами, и потому можем делать это на наиболее выгодных условиях.



– Ощущаете ли вы как отечественный производитель господдержку?

– Стараемся в основном обходиться своими силами, в рискованных проектах не участвуем. Господдержку ощущаем опосредованно, через требования, которые выдвигаются в тендерах и конкурсах.

– Насколько сильны стереотипы заказчиков в отношении отечественных изделий?

– Мы наблюдаем большую инерцию и привыкание заказчиков к уже используемым (импортным) брендам. На этапе становления отрасли ЦОДов на рынке почти не было российских производителей с изделиями хорошего качества и широкой номенклатурой. Мы очень отставали, но сейчас быстро нагоняем. Зачастую заказчику достаточно один раз самому увидеть наше изделие, например серверный шкаф, и стереотипы сразу ломаются.

– Поговорим о ваших планах.

– Мы расширяем производственные площадки. В этом году купили в Костроме еще одно здание площадью 7 тыс. кв. м для металлообработки. Сейчас делаем ремонт, устанавливаем оборудование, до конца года введем в эксплуатацию. На этой новой площадке будем производить шкафы для ЦОДов.

Для меня важно, чтобы больше потенциальных партнеров и заказчиков узнали о нас, о наших производственных площадках, наших возможностях. Хотим донести до них, что сегодня в России производятся качественные решения, которые в разы дешевле импортных и могут быть быстро кастомизированы и поставлены.

Доверие – важный элемент нашей работы. Если мы станем известны шире, то и работать будет чуть легче, да и российской продукции в каждом машзале станет больше. Долгие годы мы занимались строительством компаний. Мы созрели для мощного рывка. И в ближайшие пять лет намерены выйти на ведущие позиции на российском рынке инфраструктурных решений для ЦОДов.



www.emilink.ru
(800) 777-13-00

Гиперконвергенция и СХД: горизонты применения

Вячеслав Володкович,
генеральный директор,
«Аэродиск»

Для решения задач цифровизации компании все чаще прибегают к гиперконвергентной ИТ-инфраструктуре. Каковы возможности использования СХД в гиперконвергентных системах?

Зачем нужны гиперконвергентные системы

Традиционный подход к развертыванию ИТ-инфраструктуры предполагает сборку ИТ-систем из компонентов разных вендоров с дальнейшей настройкой их взаимодействия. Любая классическая ИТ-архитектура – это нелинейная система с множеством соединений между СХД, серверной частью и сетью. В рамках же гиперконвергентного подхода создается интегрированный комплекс по принципу «все в одном». Каждый узел кластера (сервер) содержит в одном корпусе систему виртуализации, сетевые компоненты и СХД.

Настройка или апгрейд классической ИТ-системы требуют проверки совместимости каждого компонента с остальными составляющими на уровне «железа» и ПО. Гиперконвергентные системы (ГКС) предоставляют готовую ИТ-среду «из коробки» для быстрого запуска приложений и развертывания баз данных. Настраивать взаимодействие между базовыми инфраструктурными компонентами в ГКС не нужно. При таком подходе уменьшается возможность отказа связи «железо + ПО». ГКС также проще эксплуатировать, масштабировать и модернизировать.

Гиперконвергентные решения могут служить основой для создания корпоративных ИТ-систем с нуля, а также встраиваться в существующий цифровой ландшафт предприятия в качестве вспомогательного элемента. Например, при необходимости масштабирования системы для работы с «горячими» данными использовать ГКС может оказаться дешевле, чем закупать дополнительные диски нужного объема для СХД.

Экономия времени и средств за счет изначальной совместимости компонентов ГКС может быть существенной даже на небольших проектах, не говоря уж о развертывании масштабных решений. Так, сроки проектирования ИТ-систем на базе ГКС по сравнению с традиционными архитектурами можно сократить с не-

скольких недель до дней, а апгрейд ИТ-системы может занимать буквально несколько часов.

Когда ГКС – хороший выбор?

Компаниям, проводящим цифровизацию, нет смысла наращивать свои компетенции, скажем, в СХД, целесообразнее сосредоточиться на проблемах основного бизнеса. ГКС в таком случае является оптимальным решением для экономии времени и фокусирования компетенций на ключевых рабочих задачах.

Первоочередная проблема, которую нужно решить, – выработать базовый подход к ИТ в целом и системам хранения данных в частности. Мы акцентируем внимание на СХД в данном контексте по причине постоянно растущей роли данных практически в любой сфере деятельности.

Расширенное использование цифровых инструментов в работе компаний, госструктур и частных лиц приводит к лавинообразному росту объемов данных, возникающих при их взаимодействии в онлайн и офлайн. Собранную информацию нужно не просто обрабатывать и хранить, но и делать это в соответствии с отраслевыми особенностями, требованиями регуляторов, а самое главное – экономически эффективно.

«Водораздел» между классическими и гиперконвергентными решениями в СХД проходит по следующим основным пунктам:

- Классические СХД хорошо справляются с плохо распределяемой рабочей нагрузкой (системы видеонаблюдения или масштабные транзакционные СУБД). Гиперконвергентные СХД лучше работают с такими нагрузками, когда множество задач распределяется по всем нодам системы, а не «грузит» собой один узел.
- Классические СХД приспособлены к вертикальному масштабированию и очень «не любят» горизонтальное. Гиперконвергентные СХД прекрасно масштабируются горизонтально.
- Классические СХД одинаково хорошо подходят для работы как с виртуальными, так и с фи-

зическими серверами. ГКС СХД «заточены» под виртуальные среды.

Пройдясь по этой шпаргалке, можно понять, что подойдет для решения поставленной задачи – ГКС или классическая ИТ-архитектура.

Планирование и сайзинг

Далее следует в два этапа провести планирование. Первый этап – это выработка требований к ИТ-решению, т.е. их сбор и анализ. Второй – непосредственно сайзинг и конфигурирование самого решения.

Первый этап существенно важнее второго. Требования бизнеса к ИТ-решению – та отправная точка, которая определяет развитие всего проекта. В зависимости от того, сколько времени ИТ-система может быть недоступна без причинения критического ущерба бизнесу, от необходимого режима работы, от сроков хранения бэкапов выбирают тип и конфигурацию решения.

После этого рассматривают технические требования: какой функционал нужен, какие системы на рынке его поддерживают, насколько они укладываются в бюджет и соответствуют целевым показателям производительности.

Все зафиксированные бизнес- и технические требования надо проверить. Частая ошибка на этом этапе – после начала построения решения проводить его тестирование прямо по ходу работ. Тестировать надо до финального выбора подхода к проекту. То есть сформулировали требования – и сразу же проверили их выполнение на определенном типе решения в рамках пилотного проекта.

Тестирование можно провести на ресурсах пилотной зоны внутри организации или в облачной среде. Также с просьбой организовать пилотную зону можно обратиться к интегратору или к производителю оборудования. Любой подход поможет проверить требования и на базе полученной информации разработать профиль нагрузки и определить вычислительные мощности системы.

Только после этого переходят к сайзингу, который начинается не с расчета конкретных показателей, а с выбора технологического подхода – ГКС или классическая СХД.

ГКС и СХД: взгляд изнутри

Если с традиционными СХД сталкивались многие, то особенности гиперконвергентных систем необходимо описать подробнее.

Распределенное хранилище в таком продукте позволяет объединять локальные диски серверов в пул для дальнейшего представления системе виртуализации. ГКС поддерживают дубликацию, репликацию, снапшоты и клоны, технологию стирающего кода (erasure coding), а

также предоставление ресурсов хранения для внешних систем. Современные ГКС также позволяют использовать различные протоколы доступа к хранилищу (iSCSI, NFS, SMB) и допускают развертывание в нескольких ЦОДах с формированием так называемого метрокластера (metro cluster).

Как правило, минимальное количество нод – три. Три узла необходимы для надежной работы и обеспечения отказоустойчивости. Если выйдет из строя одна нода, а две другие продолжат нормально функционировать, то с данными в ГКС СХД все будет в порядке. Выбывшую ноду можно будет спокойно заменить, не останавливая работу системы.

Если выбывают две ноды, важно иметь три копии данных. Но в этом случае запускается режим maintenance mode, когда потери придется восстанавливать вручную.

Что касается метрокластера, то ГКС могут поддерживать распределение как на уровне ЦОДов, так и ниже – вплоть до уровня стоек. Соответственно, можно распределять их по зонам, или создавая классический метрокластер, или формируя отдельные отказоустойчивые блоки. Самое главное здесь – наличие хорошей сети. В традиционных СХД ситуация в принципе аналогичная, но в ГКС этому аспекту уделяется больше внимания.


Резюме

Применимость традиционного и ГКС-подхода к практическим задачам можно представить следующим образом.

Стандартные инфраструктурные сервисы – служба каталогов, небольшие почтовые серверы, СЭД, файловые серверы, средних размеров СУБД, любые распределенные вычисления, облачные системы – хорошо ложатся на формат ГКС с точки зрения общей производительности и специфических задач СХД. А вот масштабные enterprise-системы разворачивать на ГКС смысла не имеет.

Гиперконвергентный подход прекрасно подходит для ИТ-задач филиальных сетей, когда нужно организовать стандартную отказоустойчивую инфраструктуру в каждом региональном подразделении. При этом строить в каждом филиале инфраструктуру из СХД, коммутаторов, серверов и гипервизора – долго, сложно и неудобно. Поэтому ГКС как формат «все в одном» позволяет оперативно «поднять» все необходимые ИТ-ресурсы. Далее их также просто синхронизировать и реплицировать данные из всех филиалов.

Благодаря своей динамичности ГКС хорошо решает и задачи тестовых сред: если компании нужно что-то создавать, тестировать и масштабировать, проверять совместимость с legacy-системами, то тестирование лучше проводить в ИТ-средах на базе ГКС. **ИКС**



Системы цифровизации здравоохранения: интеграционная платформа vs моноМИС

Андрей Дюков,
руководитель отдела продаж и развития,
«Нетрика Медицина»

Будущее нужно строить на фундаменте настоящего, а настоящее все еще задает банальный, но острый вопрос – почему не получается создать региональную медицинскую информационную систему с универсальной функциональностью, которой были бы довольны и пользовались все медорганизации региона?

Два подхода к информатизации регионов

В профессиональном обиходе монолитными, или моноМИС, называют медицинские информационные системы коммерческого поставщика, который монополизирует рынок МИС региона, административными мерами затрудняя медорганизациям закупку решений иных производителей. Аналогичная ситуация может складываться и с другими информационными системами медицинского назначения, например, ЛИС (лабораторными информационными системами) или ЦАМИ (центральным архивом медицинских изображений). МоноМИС и сама может включать в себя несколько отдельных решений – моноЛИС, моноЦАМИ, – не всегда до конца интегрированных между собой.

Существует и иной подход – использование интеграционной архитектуры. В этом случае главный врач, несущий ответственность за процессы внутри медицинской организации, вправе выбрать МИС, которая в наибольшей степени соответствует задачам медорганизации, ее финансовым возможностям, текущему уровню информатизации и подготовки персонала. Обмен данными между разными МИС на региональном уровне обеспечивается, например, интеграционной платформой в составе государственной информационной системы в сфере здравоохранения (ГИСЗ) региона. Интеграционная платформа задает общие для всех разработчиков МИС правила и стандарты взаимодействия. А медорганизации и главные врачи получают собственные локальные МИС и другие информационные системы медицинского назначения, которые максимально учитывают условия работы в конкретном регионе – уровни заболеваемости, летальности, обеспеченности медицинскими кадрами и т.д. Мы являемся убежденными сторонниками именно такого, интеграционного подхода.

Оба подхода применяются на практике в течение последних 10 лет, начиная еще с программы модернизации здравоохранения 2011–2013 гг. В рамках и интеграционной, и монолитной архитектуры прилагаются значительные усилия для создания ГИСЗ регионов, цифровизации амбулаторного и стационарного звена. В ряде регионов большую часть условно типовых амбулаторных медорганизаций работа моноМИС устраивает, но для стационаров и узкопрофильных медучреждений мы пока не видим давно ожидаемых успехов.

Важность нетиповых процессов

Яркий пример нетиповых процессов медорганизации приведен в книге «Управление медицинской организацией. Первые шаги» под общей редакцией Н.Н. Карякина: вновь избран-

ный главный врач решил создать централизованное отделение плановой госпитализации и все потоки госпитализации пациентов пустить через него. Для главврача это было само собой разумеющимся, но заведующие отделениями медорганизации всегда работали иначе. Мы видим, насколько по-разному могут быть выстроены процессы медицинской деятельности и насколько критична здесь роль руководителя медорганизации. При этом МИС и другие информационные системы как инструменты должны быть достаточно гибкими, чтобы поддерживать нетиповые процессы.

Интересна скорость реакции поставщиков моноМИС и локальных МИС на запросы медорганизаций с нетиповыми процессами. Хороший пример привели коллеги из областной клинической больницы (ОКБ) региона с населением около 1,5 млн человек. Местный медицинский информационно-аналитический центр, будучи оператором моноМИС, три месяца рассматривал запрос ОКБ на реализацию остро необходимой функциональности. В итоге МИАЦ и поставщик моноМИС отказали ОКБ. Через некоторое время в ОКБ внедрили собственную локальную МИС, после чего для разработки запрашиваемой функциональности понадобились лишь несколько часов: вечером сотрудники ОКБ прислали запрос, с утра нужная функция в их МИС была уже реализована. Понятно, что в условиях трансформации процессов медицинской деятельности, а особенно в условиях пандемии, когда происходит перепрофилирование крупных медицинских организаций, оперативность становится одним из решающих факторов: ожидать внедрения необходимой функциональности квартал или полгода недопустимо.

Монолитный подход спотыкается, когда сталкивается с задачами, которые выбиваются из ряда типовых. Например, с задачами специализированных стационаров, таких как институт травматологии. Да, операции. Да, стационар. Но есть склад эндопротезов, который должен с точностью до минуты поставить протез к операционному столу. И функциональность, обеспечивающая эту потребность, должна быть вплетена в МИС и начинать работать еще до поступления пациента. Подобное учреждение не согласится на упрощенную функциональность, которую ей предложат в составе унифицированной моноМИС, – главврач специализированного медучреждения захочет внедрить у себя лучшую функциональность, соответствующую потребностям медорганизации и процессам медицинской деятельности. Только в этом случае МИС будет использоваться фактически, а не формально, и приносить реальную пользу врачам и пациентам.

Совершенно различны, на мой взгляд, процессы медицинской деятельности и даже их дина-



▲ Эволюция подходов к информатизации здравоохранения

мика, например, областного онкологического диспансера и перинатального центра: онкодиспансер лечит и наблюдает пациента на протяжении нескольких лет, у перинатального центра срок – месяцы или несколько дней. Также у них различаются состав и типы данных осмотров, инструментальных, лабораторных исследований и множество другой медицинской информации о наблюдаемом пациенте. Подобные учреждения зачастую проактивны в цифровой трансформации и хотят лучших конкурентоспособных решений от лучших поставщиков. Такие клиники не согласны довольствоваться унифицированной моноМИС, решающей в первую очередь типовые задачи, без учета их профиля и специфики. Попытки же реализовать уникальную и сложную функциональность, для которой моноМИС изначально не предназначена, приводят к государственным контрактам, не дающим ожидаемого результата.

Особенности работы стационаров

Разные подходы нужны при подключении стационаров и поликлиник. Внедрение МИС в стационаре может быть технически сложнее проекта внедрения в поликлинике. Важно учитывать специфику процессов медицинской деятельности этих учреждений. В поликлиниках процессы можно охарактеризовать связями между специалистами, здесь можно говорить об информатизации отдельных рабочих мест (АРМ). В стационарах же информатизация выходит на новый уровень абстракции – взаимодействие происходит на уровне не отдельных АРМ врачей, но отделений стационара. В поликлинике процессы медицинской деятельности ведут пациента от врача к врачу. В стационаре пациент перемещается между отделениями, а далее работа с пациентом ведется уже внутри отделения. В отделениях стационара также внедряются АРМ специалистов, но затем необходимо информатизировать процессы медицинской деятельности между отделениями стационара. Умножаем сложность информатизации

отдельных АРМ стационара на сложность информатизации сквозных процессов между отделениями, получаем задачу не в разы, а на порядок сложнее, чем в поликлинике.

На практике крупные стационары предпочитают пользоваться ранее выбранными локальными МИС и не переходить на единые облачные решения. Примеров этого в России бесчисленное множество, но такие случаи нередко замалчиваются – вместо фактически используемой МИС публично указывается региональная информационная система. А на деле в облачной моноМИС либо ведется частичная регистрация пациентов для отчета по федеральным показателям записи через ЕПГУ, либо часть документов формируется вручную для отчета по тем же федеральным показателям, основанным на предоставляемых медицинских документах. Ситуация может усугубляться, когда разработчику локальной МИС организационными мерами блокируют возможность интеграции с многочисленными регистрами и реестрами. Разработчик становится своего рода изгоем, а сказывается это на врачах и среднем медицинском персонале: они вынуждены несколько раз вводить одни и те же данные в не интегрированные между собой системы.

С другой стороны, крупным поставщикам моноМИС приходится устраивать голосование на предмет того, какие запросы на разработку новой функциональности выполнять в первую очередь. Все запросы выполнить невозможно – ресурс разработки всегда ограничен и всегда в дефиците. Как вы полагаете, заявки каких регионов оказываются в приоритете? Регионов с большим населением или с большим бюджетом? Нет. Может быть, заявки регионов, которые просят об объективно необходимых и полезных доработках? Нет. Побеждают регионы, конфликт с которыми может обернуться для поставщика моноМИС теми или иными неприятностями. И зачастую нужды крупных стационаров – тех, на которых держится региональное здравоохранение, – остаются без внимания. Это печально. Чтобы двигаться в направлении цифровой трансформации, надо учитывать потребности как минимум ключевых стейкхолдеров. Нужно, чтобы крупные региональные учреждения, от которых фактически зависит здоровье граждан, были услышаны.

На пути к интеграционному подходу

В России в сферах, работающих с бюджетными деньгами, в частности в информатизации здравоохранения, не принято говорить о неудачах: каждый государственный рубль должен быть потрачен с умом и принести правильный

результат. Поэтому я был искренне удивлен, когда в 2017 г. на проводившейся нами конференции «Практическая польза региональных информационных систем в сфере здравоохранения» доктор Филип Скотт, представитель одного из британских университетов, рассказал, что в Великобритании неэффективно потратили 16 млрд ф. ст. на внедрение моноМИС, ничего в итоге не получив. Зато узнали, как точно не нужно делать.

Доктор Скотт заявил, что считает выбранный нами путь верным: он позволяет осуществлять более глубокую децентрализацию решений на уровне региона, привлекая различных поставщиков и интегрируя их между собой. Сегодня стран, которые идут по пути децентрализации, дающей возможность набирать разнообразные лучшие практики, немало. Российский же опыт цифровизации здравоохранения уникален, как уникален и сам проект – своей масштабностью, мощной финансовой поддержкой со стороны государства.

И наш опыт, и опыт коллег из разных стран мира (см. например, «Цифровое здравоохранение в Финляндии: плюсы интеграционного подхода»*) говорит о том, что информатизация здравоохранения неуклонно переходит от неуправляемого множества интеграций через моноМИС к архитектуре интеграционного оператора (см. рисунок).

Работа поставщиков моноМИС по предоставлению отдельных баз данных и прикладного программного обеспечения для каждого стационара – это промежуточный этап в переходе к полноценному интеграционному подходу. После децентрализации баз данных и прикладного ПО необходимо создать интеграционную платформу, объединяющую различные БД, идентификаторы пациентов, врачей, справочники и т.д. Затем нужно будет развивать интеграционную платформу, чтобы она соответствовала реалиям цифровой трансформации, а порой и опережала их. Предстоит создать интеграционную экосистему, в рамках которой можно будет применять лучшие практики поставщиков различных систем поддержки принятия врачебных решений, систем на основе искусственного интеллекта и других помощников врачей и среднего медицинского персонала, пациентов и руководителей здравоохранения.

Здравоохранение ожидает от компании-разработчика глубокой экспертизы с пониманием задач цифровой трансформации в быстро меняющихся условиях пандемии. Ключевой фактор – возможность выбора лучших решений, их оперативной и гибкой корректировки с учетом различных процессов медицинской деятельности.

Сегодня уже разработано множество технологий, способных ускорить цифровую трансформацию здравоохранения. Многообразие этих решений поможет интегрировать созданные информационные системы, а существующая инфраструктура должна предоставить возможность – интеграционную экосистему, чтобы потребители могли выбирать лучших. **ИКС**

*www.iksmedia.ru.

ЦИФРОВИЗАЦИЯ ЗДРАВООХРАНЕНИЯ В ЦИФРАХ

по данным Института статистических исследований и экономики знаний при ВШЭ за 2019 г.



К началу 2019 г. доступ к интернету имели медицинские организации
вели свой веб-сайт или страницу в Сети
пользовались облачными сервисами

96,5%
86,5%
36%

более **725 000** (целевой показатель 700 000)

организовано автоматизированных рабочих мест медицинских работников, подключенных к медицинским информационным системам

структурных подразделений медицинских организаций обеспечили информационное взаимодействие с ЕГИСЗ с помощью медицинских информационных систем

65,6%

подразделений обеспечили информационное взаимодействие с централизованными подсистемами государственных информационных систем (ГИС) в сфере здравоохранения субъектов РФ

24,3%

подразделений осуществляли межведомственное электронное взаимодействие с учреждениями медико-социальной экспертизы

14%

5,3% медицинских организаций предоставили доступ гражданам к электронным медицинским документам в личном кабинете пациента «Мое здоровье» на Едином портале государственных услуг

10,3 млн человек воспользовались услугами (сервисами) в личном кабинете



679 000 проведено телемедицинских консультаций (консилиумов), из них
104 000 консилиумов врачей
385 000 консультаций пациентов

40% взрослого населения страны,

или **43,7** млн чел в возрасте 15-72 лет воспользовались интернетом для записи на прием к врачу или его вызова на дом, получения сведений об оказании медицинской помощи, направления на госпитализацию, прохождения медико-социальной экспертизы (на 4 млн чел. или на 10% больше, чем в 2018 г.)



Источник: issek.hse.ru, «Цифровая зрелость здравоохранения»

Эффективный переход на отечественную виртуализацию, или Едим слона по частям

Александра Залманова, эксперт по развитию продаж отечественного ПО в ПФО и УФО, Softline

Средства виртуализации все шире используются для построения ИТ-инфраструктуры предприятий. В то же время нормативные требования подталкивают госкомпании и компании с госучастием к переходу на отечественное ПО. Как соединить эти два тренда?

В последний год к нам стали чаще обращаться с вопросами о том, как эффективно перейти на российские платформы виртуализации. Например, компании требуется виртуализировать рабочие столы или серверы, а также организовать удаленную работу сотрудников. Можно ли это сделать, используя отечественные продукты?

Если раньше системы виртуализации развивались по большей части в рамках зарубежных решений, то сегодня из-за санкционной политики опираться на такие продукты становится рискованно. Да и российские разработчики решений виртуализации уже хорошо зарекомендовали себя на рынке.

Чтобы проекты перехода на отечественные системы виртуализации были более результативны, нужно в первую очередь определить, какую задачу компания хочет решить с помощью виртуализации, и действовать поэтапно. В то же время крайне важно в процессе миграции сохранить работоспособность ИТ-инфраструктуры, не нарушить текущие критические процессы организации. Необходимо рассмотреть разные подходы, провести аудит оборудования, приложений и сервисов, выделить, что требует замены в первую очередь, а что в дальнейшем.

С чего начать

Прежде чем говорить об этапах перехода на отечественную виртуализацию, напомним, что существуют два подхода к построению инфраструктуры – классический и гиперконвергентный.

В рамках классического подхода серверы, на которых работают виртуальные машины (ВМ), через один интерфейс подключаются к остальной инфраструктуре по «меди», а через другой – по оптическим линиям к SAN-инфраструктуре и далее к СХД. Оборудование делится по типу

выполняемых задач: серверы – для вычислений, СХД – для хранения данных. В такой системе обвязка в виде блейд-серверов, в которых нет дисков, является эффективным решением для обеспечения отказоустойчивости вычислений. Недостаток классического подхода в том, что компания оказывается привязанной к производителям СХД, а в случае обрыва связи с узлом хранилища возникают риски потери инфраструктуры.

При гиперконвергентном подходе серверы и СХД объединены в одно логическое устройство, а СХД предоставлена всему виртуальному пулу серверов. Преимущества этой системы в том, что данные хранятся не на одном, а на нескольких серверах, что повышает отказоустойчивость и скорость доступа к данным. Такой архитектурой удобнее управлять, ее удобнее масштабировать, а также она позволяет развернуть полноценную систему виртуализации. К недостаткам гиперконвергентной инфраструктуры можно отнести разве что ее непривычность, поскольку в компаниях преобладает классическая инфраструктура. Однако в последнее время мы отмечаем интерес к гиперконвергенции у крупных государственных предприятий и коммерческих организаций.

Важно понимать, что речь идет о компаниях, у которых уже построена ИТ-инфраструктура. В основном классическая, реже – гиперконвергентная. Выбор ПО в данном случае будет зависеть от инфраструктуры и ее возраста. Если инфраструктура классическая, выстроена относительно недавно (не более трех лет назад) и включает в себя не только ПО, но и серверы, и при этом имеется новое оборудование, на которое было потрачено немало средств, то мы рекомендуем оставаться в рамках классической архитектуры. Если же инфраструктура



◀ Этапы перехода на новую виртуализацию

старше трех лет, оборудование и ПО давно не обновлялись, то рекомендуем выстраивать виртуализацию в рамках гиперконвергентной архитектуры.

В целом перевод компании на новую виртуализацию – сложный, объемный и довольно трудоемкий процесс. Именно поэтому мы рекомендуем проводить его поэтапно, иными словами, «есть слона по частям».

От чего зависит сложность процесса

Сложность процессов при переходе на отечественную виртуализацию зависит главным образом от количества и типов сервисов. Поэтому в первую очередь необходимо провести обследование всей ИТ-инфраструктуры и выявить сервисы, которые не являются для нее критичными.

Далее необходимо очертить пилотный контур. ИТ-оборудование в компании обычно ис-

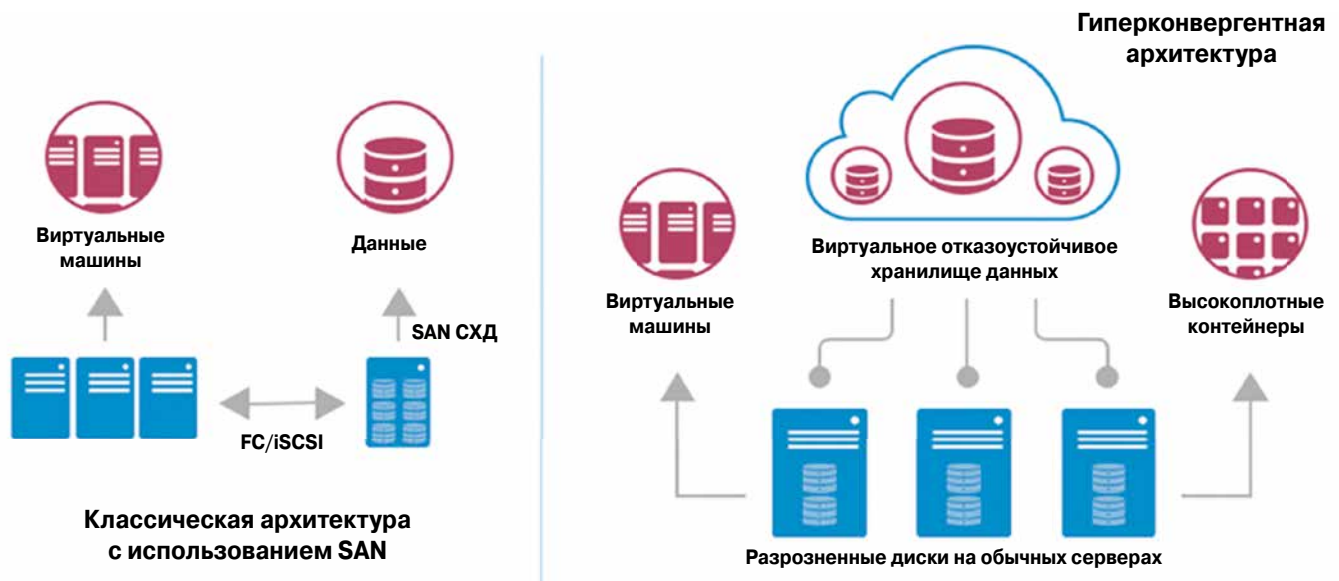
пользуется не более чем на 70–80%. Поэтому она может выделить 10% всей инфраструктуры для новой виртуализации, не приобретая для тестового развертывания новое оборудование.

В дальнейшем, успешно протестировав все сервисы в рамках пилотного контура, можно масштабировать виртуализацию, разделив эти сервисы на части и определив последовательность миграции для каждой из них.

Как правило, переход на отечественное ПО – длительный процесс, так как не все сервисы могут работать с Linux. Поэтому некоторое время в компании могут параллельно существовать два контура. При этом большая часть сервисов уже может работать на отечественной виртуализации.

Далее начинается перевод сегментов, которые требуют переноса в первую очередь. Последующие этапы зависят от размера и осо-

Перевод части существующей системы виртуализации ▼



бенностей инфраструктуры конкретной организации.

Какое ПО для виртуализации выбрать

Системы для виртуализации подбираются в зависимости от типа инфраструктуры предприятия.

Для классической архитектуры мы рекомендуем следующие решения: ПК СВ «Брест» (Astra Linux), «Альт Сервер Виртуализации», ROSA Virtualization, «Ред Виртуализация», zVIRT, Tionix. Для гиперконвергентной архитектуры лучше всего подойдут решения «Р-Виртуализация» («Р-Платформа») и ПК «Скала-Р».

Виртуализация рабочих столов и серверов

Сегодня многие организации хотят виртуализировать рабочие столы или серверы. Это необходимо, чтобы организовать удаленную работу сотрудников.

Серверная виртуализация – это механизм создания виртуального программного представления ресурсов без привязки к аппаратному обеспечению, при котором физический сервер разделяется на несколько изолированных виртуальных серверов с помощью ПО. Иными словами, есть оборудование, которое поддерживает технологии виртуализации AMD и Intel. На это оборудование устанавливается гипервизор, задачей которого является разделение физического оборудования и предоставление его виртуальной машине. VM при этом воспринимает виртуальное эмулированное оборудование как физическое.

Виртуализация рабочих столов – процесс, в принципе схожий с серверной виртуализацией. Но разница в том, что на виртуальной машине устанавливается гостевая операционная система, которая будет использоваться как обычный компьютер. Когда виртуальная машина работает в ЦОДе, пользователю нужно взаимодействовать только с той «картинкой», которую он видит на своем планшете, ноутбуке или персо-

нальном компьютере, а все вычисления будут производиться в серверной.

Терминальный доступ и VDI

Еще один вопрос, который часто волнует компании, – обеспечение терминального доступа или VDI. Многие путают эти два понятия. В чем разница?

Терминальный доступ (Terminal Services) – это среда, в которой пользователи работают совместно на виртуальной машине, находящейся в серверной операционной системе. Он более удобен при проблемно ориентированном подходе и совместной работе сотрудников. Среди программных решений можно отметить «Термит».

VDI – это отдельная виртуальная машина для каждого пользователя, работающая с клиентской операционной системой. Технология изолирует пользователей друг от друга, поэтому VDI лучше применять в средах, где важна конфиденциальность информации. Для решения этой задачи может быть использовано следующее программное обеспечение: «Скала-Р Виртуальное Рабочее Место», ROSA Virtualization, Tionix VDI, Termidesk (Astra Linux) и др.

VDI позволяет сэкономить на оборудовании для сотрудников, особенно при решении «тяжелых» графических задач, в частности при работе с 3D-графикой.

Недавно Softline совместно с НТЦ ИТ РОСА провела тестирование возможностей VDI ROSA Virtualization при использовании виртуальных рабочих мест в сценариях с «тяжелыми» графическими CAD/CAM-приложениями. Тестирование прошло успешно, подтвердив заявленный функционал взаимодействия с графическими картами и его высокое качество для каждого рабочего места.

Можно ли самостоятельно перейти на отечественную виртуализацию?

Да, можно. Компании, как правило, имеют опыт эксплуатации зарубежных сред виртуализации. Однако переход на отечественную виртуализацию требует знаний и опыта миграции, который у большинства еще не наработан. Также важно не только правильно подобрать продукт, но и рассчитать ресурсы оборудования и лицензии.

Поэтому мы рекомендуем подключать к этой задаче опытного ИТ-интегратора, который поможет минимизировать риски и сроки перехода на новую систему виртуализации. Поскольку в настоящее время нормативные требования к приобретению отечественного оборудования скорректированы, как никогда важно владеть информацией и в области виртуализации. **ИКС**



Распределенные вычисления и надежность гибридных сред

Гибридная мультиоблачная модель и распределение вычислительных ресурсов по платформам нескольких провайдеров дают компаниям возможность обеспечить интегральную надежность своей ИТ-инфраструктуры.

Распределенные системы, выполняющие параллельные вычисления на нескольких узлах, помогают агрегировать ресурсы для создания эластичных производительных вычислительных сред и решения ресурсоемких задач. При создании распределенных систем компании, как правило, прибегают к гибридной модели: критичные сервисы размещают на локальной (собственной) инфраструктуре и/или в частном облаке, а при необходимости подключают дополнительные сегменты в публичных облаках для некритичных сервисов и резервного копирования данных.

Зачем нужна распределенная ИТ-архитектура

Требования бизнеса (расширение филиальной сети, увеличение числа используемых сервисов, неравномерная нагрузка) подталкивают компании к гибридной модели. Эта модель помогает снизить капитальные затраты и повысить гибкость ИТ-архитектуры за счет возможностей публичных облаков. При этом она позволяет сохранить высокую надежность и безопасность, присущие локальной инфраструктуре.

Переход к гибридной инфраструктуре целесообразен, если она решает следующие задачи, стоящие перед бизнесом.

- **Оптимизация затрат.** К публичным облакам компании обращаются, когда локальная инфраструктура нуждается в модернизации, но одновременно выделить на нее крупную

сумму нежелательно или невозможно. Бывает, что дешевле начать использовать полностью новый инструментарий, чем налаживать старый в новом окружении. Тогда разумно задействовать публичное облако в качестве «перевалочного пункта» на пути к облачной модели потребления ИТ-услуг.

- **Гибкое масштабирование.** Публичное облако помогает повышать производительность всей вычислительной системы пропорционально нагрузкам и компенсировать ограничения локальной инфраструктуры. Благодаря публичной части гибридная модель дает возможность оперативно подключать удобно масштабируемые ресурсы. Она позволяет компаниям с сезонной нагрузкой, быстрорастущим стартапам и организациям, которые реализуют временные проекты, динамично менять потребление вычислительных мощностей.

- **Надежность.** Используя гибридную модель, легко распределять нагрузку по облакам: некритичные сервисы с нестабильной нагрузкой размещать в публичном облаке, а «ядро» инфраструктуры с повышенными требованиями ИБ – в частном. Резервирование вычислений на нескольких площадках уменьшает вероятность простоя сервисов и абсолютной потери доступности. При наличии настроенного резервного копирования или аварийного восстановления легко переключиться на резервную площадку в случае форс-мажора на основной. При этом провайдеры часто предоставляют техническую поддержку и помогают

Александр Бытин,
заместитель
руководителя
отдела
пресейла,
«Онланта»
(ГК ЛАНИТ)

обслуживать гибридную инфраструктуру, что также снижает риски простоев.

Как перейти от локальной инфраструктуры к гибридной

Если компания собирается использовать облако, необязательно переносить туда всю ИТ-инфраструктуру сразу. К облакам привыкают постепенно. Чтобы «распробовать» облака, можно для начала собрать портфель из SaaS-сервисов. ПО из облака подключается опционально и помогает поддерживать новые направления бизнеса или временные проекты.

При внедрении в компании облачной стратегии прежде всего ИТ-специалисты проводят инвентаризацию ИТ-ресурсов и сервисов, ранжируя их по уровню критичности. Затем оценивают срок полезного использования (СПИ) локальной инфраструктуры и разрабатывают целевую модель потребления облаков. В зависимости от СПИ создают план перехода в облако. Мощности локальной инфраструктуры могут служить резервной площадкой в процессе миграции.

Так компания переходит к гибридной модели: размещает ИТ-ресурсы в нескольких ЦОДах провайдера (в частном облаке разворачивается основная площадка, в публичных – резервные площадки для бэкапа и некритичные сервисы). За счет географического распределения ИТ-ресурсов качественно повышается катастрофоустойчивость бизнеса и надежность инфраструктуры.

Однако это не предел. ИТ-ресурсы можно распределить между несколькими провайдерами и

повысить надежность не только технически, но и организационно.

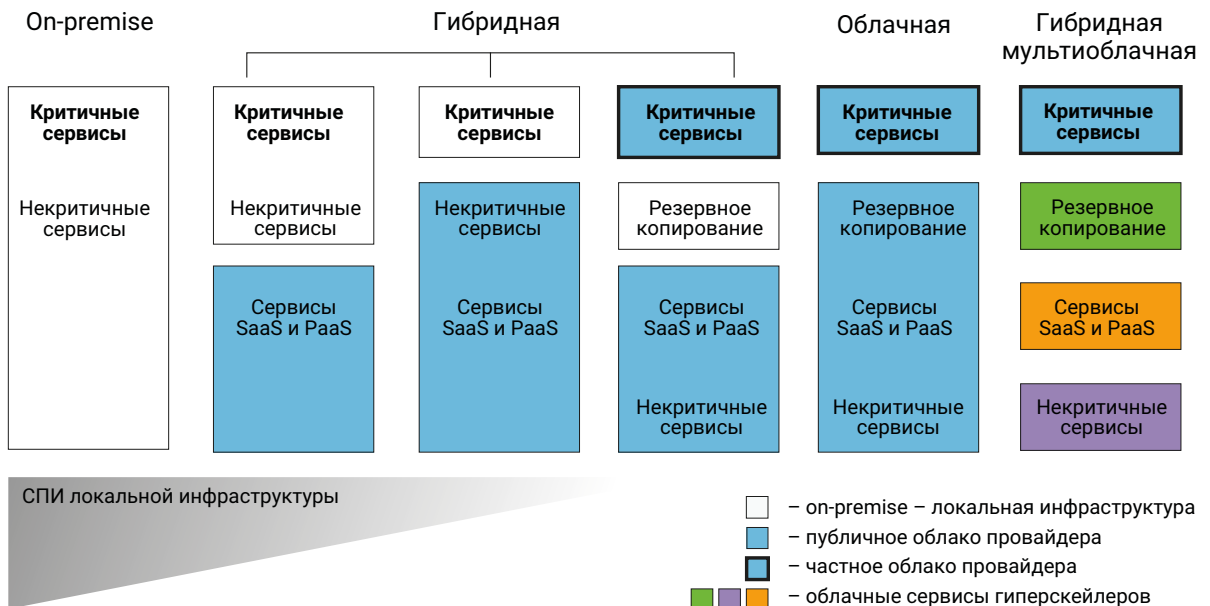
Сколько вычислительных сред на самом деле нужно

Если компания распределяет свои ИТ-ресурсы между площадками нескольких провайдеров, она становится пользователем мультиоблачной инфраструктуры. При мультиоблачном подходе бизнес может привлекать облачные платформы, ПО, технологии, экспертизу от нескольких игроков облачного рынка и оптимально делить свой ИТ-бюджет между ними. Компании идут в мультиоблако прежде всего за новыми инструментами, гибкостью функционала и оперативностью выделения ресурсов. Таким образом удается собрать в одном проекте лучшие решения на рынке за приемлемую цену. Организации арендуют частное облако (основную площадку) у одного провайдера, резервную площадку – у другого, а публичные ресурсы размещают в облаке гиперскейлера* (см. рисунок).

Мультиоблака помогают организациям разнести корпоративные сервисы по структурным подразделениям: сотрудники центрального офиса могут работать со служебными файлами в частном облаке на стороне провайдера, а публичные сервисы других провайдеров (в том числе гиперскейлеров) использовать для резервного копирования, размещения сервисов для работы филиалов и пользовательских приложений.

Некритичные сервисы и сети доставки контента компании часто распределяют по не-

Эволюция ИТ-инфраструктуры с постепенным увеличением доли использования облаков ▶



*Выделение гиперскейлеров – поставщиков глобальных облачных сервисов, таких как AWS, Alibaba Cloud, Microsoft Azure, «Яндекс Облако», Mail.ru Cloud Solutions и т.п., – в отдельную категорию обусловлено масштабом и особенностями архитектуры их дата-центров, а также широкой номенклатурой предоставляемых сервисов – Прим. ред.

скольким дата-центрам исходя из регионально-го принципа, чтобы обеспечить близость вычислений к локальным пользователям. Инфраструктура, представляющая собой «паутину» из дата-центров разных поставщиков, обеспечивает более надежное резервирование систем. Так, в случае сбоев в дата-центре одного из провайдеров работу с системой в данном регионе можно переключить на соседний ЦОД другого. Техподдержка в таком случае также распределена по провайдерам и часовым поясам, что удобно для организации непрерывной работы инфраструктуры.

Компании, предоставляющие SaaS-сервисы (по подписке из облака), тоже стали использовать платформы разных провайдеров, дата-центры которых разнесены географически. Это помогает повысить надежность работы сервисов, снизить сетевые издержки, приблизить вычисления к пользователям и обезопасить бизнес на случай проблем на стороне кого-либо из провайдеров.

Диверсификация облачных сред позволяет повысить надежность работы инфраструктуры, а гибридное мультиоблако – выстраивать бизнес-процессы, исключая техническую и экономическую зависимость от единственного поставщика облачных услуг.

Гибридное мультиоблако – архитектура с интегральной надежностью

На первый взгляд может показаться, что обеспечить стабильную работу в мультиоблаке сложнее, поскольку контроль децентрализован и необходимо дополнительно заботиться о совместимости платформ, что также влияет на отказоустойчивость. Но если строить инфраструктуру с поддержкой провайдера мультиоблака (т.е. игрока, который берет на себя ответственность за весь проект), задача сильно упрощается, поскольку подход к тесной совместимости платформ гиперскейлеров уже заведомо реализован и обкатан на его стороне. Работа с таким провайдером позволяет достичь сквозной надежности гибридных моделей архитектуры.

Гибридная модель обеспечивает надежность инфраструктуры. Но распределяя вычислительные задачи по разным провайдерам, ее можно повысить еще больше и дополнительно подстраховаться не только на техническом, но и на организационном уровне. Разнесение ИТ-ресурсов по дата-центрам до трех разных провайдеров может качественно повысить уровень отказоустойчивости. А вот дальнейшее подключение дополнительных площадок повлияет на надежность уже незначительно. С помощью мультиоблака можно повысить катастрофоустойчивость и непрерывность бизнеса, сделав надежность интегральной (кумулятивной).

Рассмотрим, как меняется уровень надежности в зависимости от архитектуры облака.

Надежность облака провайдера. Доступность сервисов фиксируется в соглашении об уровне обслуживания (SLA) и отражает гарантируемое время работы инфраструктуры без простоев в год. Нижняя планка у современных провайдеров дата-центров, сертифицированных по Tier III, находится на уровне 99,99%. Такой уровень гарантирует, что простой сервисов в течение года не превысит 53 минут.

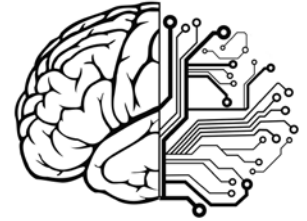
Надежность гибридного облака. За счет дублирования ресурсов в двух или более ЦОДах, каждый из которых гарантирует определенный уровень отказоустойчивости, влияние технических рисков на бизнес-процессы становится еще меньше. Дата-центры страхуют работу друг друга. Многие провайдеры предлагают услуги резервного копирования данных (BaaS) и аварийного восстановления (DRaaS) на базе нескольких своих ЦОДов.

Надежность гибридного мультиоблака. Распределив ресурсы по платформам нескольких провайдеров, можнократно увеличить резерв отказоустойчивости и предотвратить внезапную потерю данных. В случае системных сбоев или глобальных проблем на стороне одного из провайдеров работу мультиоблачной архитектуры можно переключить на резервное облако другого.

Провайдеры начинают объединяться с гиперскейлерами и предоставлять мультиоблачную архитектуру в качестве услуги в формате «единого окна». Провайдер мультиоблака пропускает через себя все процессы взаимодействия заказчика с облачными платформами, обеспечивает мониторинг всей архитектуры, а также сквозной контроль качества и информационной безопасности. Влияние технических и ИБ-рисков сводится к нулю – ни авария в дата-центре, ни DDoS-атака на стороне одного из провайдеров не парализуют работу инфраструктуры заказчика полностью. Гибридная мультиоблачная архитектура позволяет повысить надежность сервисов путем устранения единой точки отказа.

При переходе к новым этапам цифрового развития бизнеса гибридная облачная модель – незаменимый помощник. Она дает компаниям возможность использовать прогрессивные ИТ-решения здесь и сейчас, не мучаясь выбором между затратами, функциональностью и надежностью. Все ключевые параметры инфраструктуры сохраняются, а приятным бонусом становится общее повышение гибкости бизнес-процессов, связанных с ИТ. Так гибридная модель и распределение вычислительных задач между несколькими провайдерами помогают бизнесу стать более гибким и делать взвешенные шаги на пути к цифровой трансформации. **ИКС**

Искусственный интеллект в видеоаналитике. Реальные возможности



Алексей Новак,
инженер
комплексных
решений, Axis

Используя технологию машинного обучения для аналитической обработки видеоизображений, организации действительно смогут вывести свою систему безопасности на новый функциональный уровень – но, вероятно, не так, как они представляют себе это сейчас.

Искусственный интеллект – просто хорошая имитация

Применяемый в видеоаналитике искусственный интеллект в общих чертах можно описать как алгоритм машинного обучения, который обрабатывает видеоизображения или фотографии и распознает объекты на них, используя комбинации существующих визуальных характеристик. В этом, наверное, и коренится львиная доля заблуждений: мы привыкли воспринимать «интеллект» в контексте человеческого интеллекта, основанного на сознании, мышлении, креативности, – и стремимся наделить машину теми же качествами. К сожалению или к счастью, искусственный интеллект применительно к машине – это только имитация человеческого мышления. Он действует не самостоятельно и свободно, а лишь с помощью тех алгоритмов, которые в машину заложили. В случае глубокого обучения алгоритмы (нейросети) создают новые знания на основе уже полученного и проанализированного материала.

Иными словами, научить машину обрабатывать изображения нетрудно, но заставить ее мыслить как человек и безошибочно распознавать объекты гораздо сложнее. Первая сложность заключается в создании большого объема

релевантных данных. Пояснить это можно на простом примере. Допустим, мы загрузили изображение кошки и попросили машину воспринимать все похожие объекты как кошек. Но что будет, если машине предъявить кошку со стороны хвоста, кошку в траве, бегущее животное или только его голову? Для точного распознавания всех кошек алгоритму потребуется иметь как можно больше входных данных, вариаций одних и тех же объектов, а также признаков, по которым можно отличить кошку, например, от собаки или лисы. Более того, если кошка на какой-то части выборки будет случайно маркирована как собака, система в рабочем режиме может повести себя неадекватно.

Программа обучения

Разработка аналитического приложения на основе машинного обучения состоит из нескольких этапов. В первую очередь необходимо четко определить цель приложения: скажем, распознавание людей или животных, транспортных средств и номерных знаков на них. Ведь даже для того, чтобы правильно считать номерной знак, система должна идентифицировать объект как транспортное средство (отличить его, например, от человека, несущего табличку с цифрами) и найти на нем область, где этот знак расположен.

Один из самых трудоемких процессов – сбор большого объема данных, отдельных снимков и видеоматериалов и их аннотирование. Как правило, при машинном обучении оперируют несколькими тысячами изображений, а при глубоком обучении – миллионами. Аннотирование – это классификация и маркировка объектов. С целью исключения ошибок оно выполняется в основном вручную. Затем аннотированные данные загружаются в обучаемую модель, и она итеративно изменяется и оптимизируется до тех пор, пока не станет соответствовать поставленным задачам.

Соотношение технологий искусственного интеллекта, машинного и глубокого обучения ▼



На определенных этапах обучения, а также по его окончании модель тестируют сперва в лабораторном режиме (загружают ранее не использованные данные и наблюдают за реакцией), а потом в условиях реальной нагрузки. Если результат проверки оказывается неудовлетворительным, то весь процесс, включая сбор обучающих данных, приходится начинать заново. Если же модель соответствует ожиданиям, переходят к этапу развертывания. В ходе этого этапа делают выводы и прогнозы, касающиеся выполнения обученной моделью своих функций в рамках системы видеонаблюдения с соответствующей производительностью.

Чего мы не могли себе представить

Аналитике на основе искусственного интеллекта специалисты в области видеонаблюдения уже находят самые разные применения. Типичный пример – более точное распознавание транспортных объектов в системах управления трафиком, идентификация грузовиков, автобусов, автомобилей и мотоциклов, уменьшение количества ложных срабатываний (тревожных сигналов). Аналитический модуль также может зафиксировать движущийся объект на запрещенной для прохода территории, распознать в нем человека (а не животное) и выдать предупредительный сигнал.

Однако этим возможности машинного обучения не ограничиваются. Более того, это только начало. С развитием технологии, особенно на уровне глубокого обучения, мы сможем добиться от системы видеонаблюдения еще более интересных вещей. Система способна в течение долгого времени накапливать, обрабатывать и анализировать огромный объем данных – такой анализ физически невозможно провести вручную – и выявить некие закономерности и аномалии в контролируемых процессах, о которых мы и не подозревали. Использовать такие системы можно не только для охраны, но и для мониторинга условий труда, улучшения сервиса, анализа бизнес-процессов, прогнозирования инцидентов (например, задымлений).

К слову, в США медицинский алгоритм глубокого обучения Etemadi научился самостоятельно диагностировать рак легких гораздо точнее и на более ранних стадиях, чем если бы просто сопоставлял загруженные в модель снимки. Даже по этому примеру можно судить о том, насколько важны для общества исследования в области искусственного интеллекта, глубокого обучения, видеоаналитики, машинного зрения.

Ограничения и перспективы видеоаналитики

Очевидно, что какую бы задачу видеоанализа на базе искусственного интеллекта мы ни рас-

сматривали, обучение модели и ее работа должны основываться на наборе данных хорошего качества. Упомянутая выше медицинская система оперирует снимками компьютерной томографии, сделанными с высоким разрешением. Обычно же нам приходится иметь дело с видеокameraми и сценариями, которые не позволяют аналитической системе проявить весь заложенный в нее потенциал.

Так, качество изображения зависит от расположения камеры, ее разрешения и светочувствительности, освещения и наличия хорошей подсветки в ночное время, воздействия внешних факторов – таких как падающие листья, дождь или снег. На точность распознавания влияют расстояние от камеры до объекта, скорость и направление его движения, а также настройка параметров записи. Известны случаи, когда камера имела высокое разрешение, но все равно упускала часть объектов из виду – просто потому, что система анализировала кадры, сделанные с низкой частотой. Возможно, для полноценной работы видеоаналитики камеру придется настроить на непрерывную съемку, без какой-либо фильтрации исходной записи. Разумеется, нельзя недооценивать и постоянное обслуживание устройств, поскольку обычная грязь или паутина (бывает и такое) на объективе делают работу камеры бесполезной.

Многое зависит от производительности системы и качества сети, которая должна быть способной без задержек и сбоев передавать видеопоток. Сегодня, впрочем, мы больше ориентируемся на периферийную аналитику, когда вычисления проводятся «на борту» камеры, а на сервер отправляется уже результат анализа – метаданные. Используемые камерой алгоритмы машинного обучения требуют от устройства больших вычислительных ресурсов. Нужная производительность достигается с помощью графических процессоров с особой архитектурой ядра и дополнительных специализированных модулей обработки данных с поддержкой технологий машинного и глубокого обучения.

Видеоанализ на основе технологий искусственного интеллекта и машинного обучения – несомненное будущее отрасли видеонаблюдения. Он даст возможность расширить функциональность и область применения систем видеонаблюдения, автоматизировать и качественно улучшить многие бизнес-процессы. Особую роль будет играть периферийная аналитика – она позволит в условиях потребления все большего объема данных оптимизировать системы хранения и снизить нагрузку на сетевую инфраструктуру. **ИКС**



Аутентификация на раз-два

Николай Носов

Двухфакторная аутентификация – необходимое звено защиты от кибератак, а предложение ее по сервисной модели – перспективное направление развития услуг облачных провайдеров.

Однофакторная аутентификация не спасает

Лет десять назад Банк России озаботился информационной безопасностью подотчетных финансовых организаций. Под давлением регулятора банкам пришлось заняться выполнением многочисленных требований к уровню защиты. Прежде всего – разработать и реализовать политику использования паролей.

Председатель правления банка, в ИТ-отделе которого я тогда работал, гордо заявил, что у него сложный пароль – пять единиц, а у его заместителя только четыре. Не намного лучше обстояло дело и у сотрудников. На основе рекомендаций ЦБ я разработал политику парольной защиты и добился утверждения ее правлением. Потом было много негодования, когда система требовала придумать новый пароль, причем с прописными буквами, цифрами и служебными символами, еще больше – когда выяснилось, что пароль теперь нужно менять каждые две недели. Но на все претензии был ответ – утвержденная правлением бумага.

Второе требование политики – никому, в том числе коллегам по работе, не сообщать свой пароль и уж тем более не прикреплять скотчем к монитору бумажку с подсказкой. Требование очевидное, но многие относились к нему несерьезно. Впрочем, недолго. После закрытия подмосковного отделения в головной офис перевели операционистку, мать-одиночку с двумя приемными детьми – руководство не решилось выбросить ее на улицу. Но женщину почему-то невзлюбили московские барышни. В один прекрасный день, когда она отлучилась с рабочего места, с ее компьютера сделали проводку по снятию крупной суммы денег клиента. Это была не кража – деньги перевели на счет налоговой инспекции, но вернуть их оттуда было сложно. Фактически клиент на неопределенное время потерял крупную сумму и был в бешенстве. Женщина плакала, говорила, что не ошибалась, не делала эту проводку, но доказать ничего не могла. Рабочее место ее, вход в систему сделан под ее паролем, а камеры смотрели только на посетителей, поэтому доказать, что кто-то во время ее отсутствия сел за стол, было невозможно. В любом случае вина за утечку пароля лежала на ней, так что уволили без колебаний.

Вывод: люди не хотят придумывать сложные пароли и постоянно их менять. Предпочитают запомнить один простой пароль и использовать во всех случаях. Даже если их заставить, они склонны сообщать пароль другим или записывать его в местах, доступных для посторонних. Поэтому защита только паролем – однофактор-

ная аутентификация – в большинстве случаев неэффективна.

Цифровая трансформация и пандемия

В те годы, когда банк занялся защитой периметра безопасности, проблема дискредитации паролей еще не стояла так остро. В конце концов, прежде чем войти в информационную банковскую систему, надо было попасть в здание. Но процессы цифровой трансформации привели к размытию периметра безопасности. Еще больше обострил проблему массовый переход на удаленную работу из-за пандемии.

При удаленной работе, использовании распределенных, в том числе мультиоблачных, систем возрастают риски перехвата информации по каналам связи. Например, злоумышленники могут перехватывать пароли, взломав Wi-Fi роутер, или перехватить беспроводную передачу, скажем, с помощью утилиты Airodump-ng, а затем практически в режиме реального времени дешифровать трафик WPA2 с помощью sniffера (анализатора трафика) Wireshark.

Согласно отчету киберотдела ФБР, выпущенному в марте 2020 г., киберпреступники все чаще атакуют организации, использующие облачные почтовые службы. Получив доступ к корпоративной почте, хакеры направляют платежи поставщиков и клиентов на свои банковские счета. За последние пять лет убыток американского бизнеса от взлома деловой почты составил \$2,1 млрд.

Можно и нужно защищать каналы с помощью шифрования, использовать различные криптошлюзы, протоколы защиты сетевого трафика на уровне IP (IPsec), но этого мало. Нужен еще как минимум один фактор, по которому можно аутентифицировать (проверить подлинность) пользователя. Двухфакторная аутентификация значительно повышает безопасность доступа к системе. Есть решения, в которых факторов проверки больше двух, поэтому в общем случае говорят о многофакторной аутентификации (MFA).

Как считают в Google, даже одна из самых слабых форм двухфакторной аутентификации – двухэтапная проверка с помощью текстовых SMS-сообщений – может остановить 100% автоматических атак, 96% массовых фишинговых атак и три четверти целевых атак (рис. 1).

По словам директора по безопасности идентификационной информации Microsoft Алекса Вайнерта, еще в прошлом году каждый месяц в среднем компрометировалось более 1,2 млн корпоративных учетных записей Microsoft. Из них 99,9% не имели многофакторной аутентификации.



Виды двухфакторной аутентификации

Отправка одноразовых паролей через SMS долгое время была самым популярным способом двухфакторной аутентификации. В России она таковой и остается. Однако за рубежом этот способ не считается надежным, а Национальный институт стандартов и технологий США даже призвал от него отказаться. Дело в том, что по-прежнему широко применяемый в мобильных сетях сигнальный протокол SS7 фактически не имеет защиты и в настоящее время безнадежно устарел. SMS не шифруются при передаче. Подтверждающее транзакцию SMS-сообщение можно перехватить с помощью развернутой вблизи жертвы фальшивой базовой станции (фемтосоты). А можно договориться с нечистоплотным или доверчивым сотрудником мобильного оператора о выпуске новой SIM-карты с номером телефона жертвы взамен «утраченной». Наглядный пример опасности использования сетей общего пользования – инцидент, произошедший в 2017 г. в Германии, когда хакеры, перехватывая SMS-сообщения, смогли обойти двухфакторную аутентификацию и украсть деньги с банковских карт.

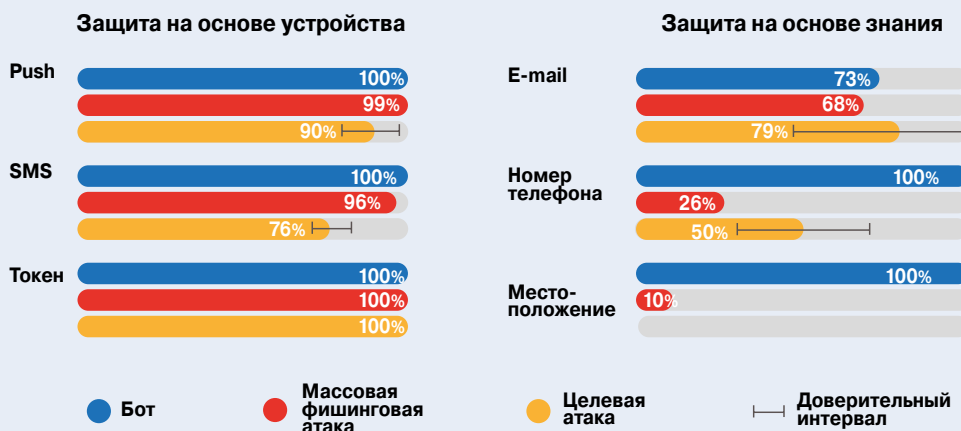
Подтверждение через электронную почту также по-прежнему широко применяется на практи-

ке. Конечно, и почту можно взломать, зато метод прост и удобен, более того, можно послать ссылку для входа в один клик без повторного ввода логина и пароля. Безопасность – компромисс между надежностью, стоимостью и удобством. Если потери из-за потенциального взлома невелики, то предпочтение можно отдать удобству. Например, если на конференцию сможет зарегистрироваться и пройти посторонний человек, то это лучше, чем если из-за сложностей регистрации на нее не сможет попасть целевая аудитория.

По данным сервиса Duo Security, позволяющего организовывать двухфакторную аутентификацию, самыми популярными способами аутентификации в США и Великобритании в 2019 г. стали push-уведомления. Приложение-аутентификатор отправляет пользователю сообщение при каждой попытке входа в систему. Ответ поступает, как правило, на расположенный в облаке сервер, разрешающий или запрещающий доступ к службе. Приложения часто показывают IP-адрес или предполагаемое местоположение человека, пытающегося войти в учетную запись. Удобно, что аутентификация осуществляется одним кликом – подтверждением правомерности входа.

Местоположение человека может служить дополнительным фактором проверки. Если прове-

Рис. 1.
Защищенность аккаунта при разных способах аутентификации



Источник: security.googleblog.com

ряемый пользователь раньше не посещал страну, из которой пытается войти в систему, то это как минимум повод для беспокойства. Подход уже используется в банках. Например, мне перезвонили из новосибирского процессингового центра, когда по карточке оплачивал аренду машины в Камеруне. Некоторые финансовые организации запрещают вход в свою систему из стран, где пользователь не планирует появляться. Для многих американцев это Россия и Китай. По данным Duo Security, в пятерку стран, автоматически блокируемых системами аутентификации, также входят США, Индия и Франция.

Для восстановления украденного пароля имеет смысл привязывать к аккаунту номер телефона. Взломают аккаунт в «ВКонтакте», начнут рассылать от вашего имени просьбы о материальной помощи – можно сбросить пароль и ввести новый с помощью телефона.

Один из наиболее безопасных методов двухфакторной аутентификации – токен. Чтобы хакер смог получить доступ к защищаемому ресурсу, токен придется украсть. Токены могут генерировать одноразовые пароли или работать как USB-ключи, открывающие при подключении к компьютеру доступ к учетной записи, на которую они зарегистрированы. Токены широко применяются для защиты наиболее ценной информации, чаще всего в государственном секторе и финансовых отраслях.

Вводить пароли или переключать токены неудобно. Есть упрощенный вариант двухфакторной аутентификации – сеточная. Пользователю предлагается матрица ячеек, содержащих случайные символы, в которой он выбирает шаблон персональной идентификации – последовательность ячеек в одном ему известном порядке, например в форме буквы Z. Система запоминает шаблон пользователя и в следующем сеансе предлагает новый набор случайных чисел. Вход разрешается, если последовательность символов вводится в соответствии с наложенным шаблоном (рис. 2).

Другой способ упрощения работы связывающий с биометрией. Для разблокирования экра-

Облачная двухфакторная аутентификация, особенно для доступа к инфраструктуре, развернутой в облаке, предпочтительнее. Связность приложений в облаке, в том числе с сервисом аутентификации, исключает проблемы доступа к on-premise-инфраструктуре компании.



Михаил Соловьев, директор по развитию продуктов, DataLine

на смартфона уже давно используют отпечаток пальца. Можно подключить распознавание голоса клиента и его лица во время онлайн-диалога с оператором. В России в этом направлении активно работает Сбер. Все это тоже факторы аутентификации, существенно повышающие сложность взлома.

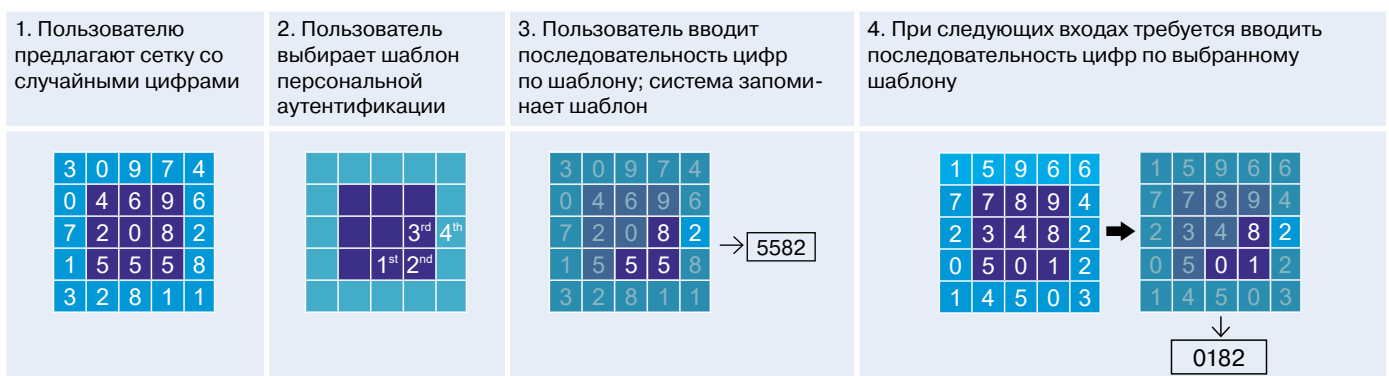
Способы реализации двухфакторной аутентификации

Организовать двухфакторную аутентификацию можно как с помощью on-premise-решения, так и с помощью облачных сервисов. Такие услуги оказывают и облачные провайдеры, и вендоры по модели SaaS. Однако SaaS-сервисы двухфакторной аутентификации от вендоров часто предоставляются из дата-центров, расположенных за пределами нашей страны, что создает дополнительные риски, например, из-за возможных блокировок Роскомнадзора. Так что для бизнеса это, как правило, наименее надежный вариант.

Классический вариант организации защищенного VPN-канала из офиса клиента до облака недостаточен в условиях размытия периметра безопасности, а тем более при удаленной работе. Да и использование одного канала на всех негативно сказывается на производительности.

Альтернативный вариант – доступ из любой точки к вычислительным ресурсам по каналу, поддерживающему протокол удаленной работы RDP и защищенному двухфакторной аутентификацией из облака (рис. 3). Например, кли-

Рис. 2. Принцип работы сеточной аутентификации ▼



Источник: Thales



Станислав Мирин,
ведущий консультант, iKS-Consulting

Стоимость данных растет, как и вложения в их защиту. Развитие сервисов безопасности из облака (SECaaS) – тренд российского рынка последних лет. Востребованность двухфакторной аутентификации будет повышаться вместе со спросом на остальные облачные услуги, так что перспективы у этого направления хорошие.

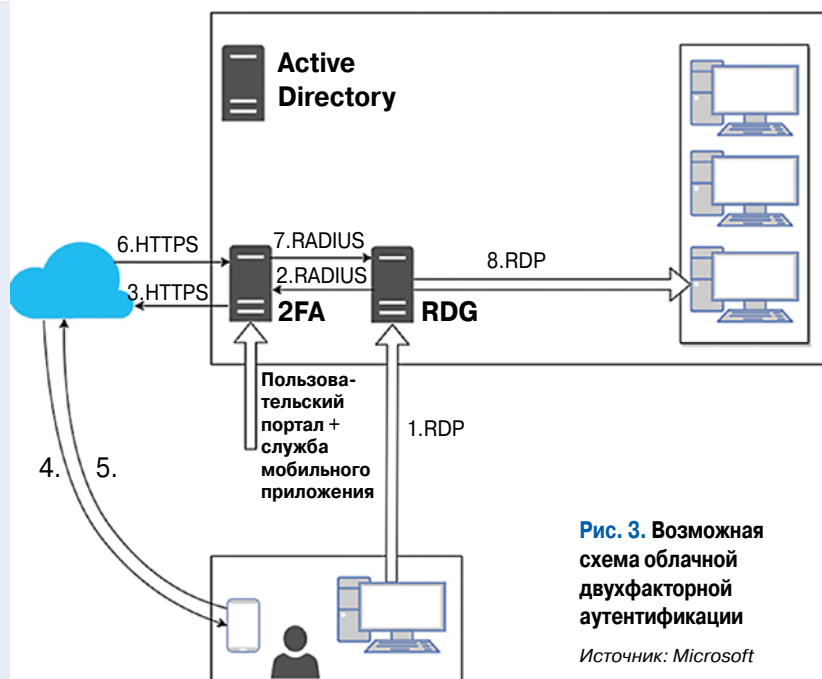


Рис. 3. Возможная схема облачной двухфакторной аутентификации

Источник: Microsoft

ент обращается по RDP к шлюзу Remote Desktop Gateway (RDG), который авторизует пользователя по логину и паролю. RDG-сервер по протоколу аутентификации RADIUS запрашивает подтверждение авторизации у развернутого на отдельной виртуальной машине сервера двухфакторной аутентификации. В зависимости от выбранного способа аутентификации 2FA-сервер звонит, отправляет SMS или посылает запрос в мобильное приложение. Пользователь подтверждает или отклоняет запрос на предоставление доступа. 2FA-сервер возвращает результат второго этапа аутентификации серверу RDG. Сервер 2FA может развертываться в облаке или устанавливаться на инфраструктуре заказчика (on-premise).

Российские облачные провайдеры чаще разворачивают двухфакторную аутентификацию как управляемый сервис в облаке, беря на себя работу по сопровождению и администрированию системы. Такие услуги особенно удобны для кли-

ентов, инфраструктура которых размещается в облаке провайдера, например, в сегменте облака, защищенном согласно требованиям регулятора о защите персональных данных. «Мы за клиента управляем сервером двухфакторной аутентификации. По сути, это наш сервер, на котором мы управляем аутентификацией клиентов и защищенность которого обеспечиваем. А клиент только заводит и удаляет учетные записи», – пояснил директор по развитию продуктов компании DataLine Михаил Соловьев.

По данным эксперта, в целом среди бизнес-пользователей облачных сервисов DataLine приобретают двухфакторную аутентификацию (отдельно или в числе других сервисов) около 10%, а среди тех, кто работает с облаком, защищенным согласно требованиям 152-ФЗ, доля пользователей сервиса аутентификации достигает 100%.

Выбор решения

На какой системе двухфакторной аутентификации есть смысл остановиться облачным провайдерам, чтобы организовать безопасный удаленный доступ своим сотрудникам и предлагать это же решение клиентам как услугу? При выборе конкретных продуктов целесообразно проанализировать ряд параметров:

- ▶ эффективность (степень снижения риска несанкционированного доступа);
- ▶ соответствие регуляторным требованиям;
- ▶ стоимость владения системой;
- ▶ удобство для пользователя;
- ▶ интегрируемость с бизнес-приложениями;
- ▶ быстроту развертывания;
- ▶ гибкость и масштабируемость при изменении числа пользователей.

Важно отслеживать попытки аутентификации, включая данные об IP-адресах и странах, занесенных в «черный» список. Хорошо, если провайдер может автоматически предупреждать администраторов о подозрительных событиях, таких как использование нового устройства или вход в систему из неожиданного места.

Также стоит обратить внимание на модель лицензирования пользователей (с ежемесячной или годовой оплатой, оплатой за число клиентов или число аутентификаций), на то, привязаны ли лицензии к одному идентификатору пользователя или могут передаваться по мере необходимости, на надбавки за дополнительные устройства и стоимость доставки уведомлений для разных факторных методов.



При сегодняшней интенсивности атак на информационные системы двухфакторная аутентификация – необходимое условие защиты, и компании начинают это понимать. **ИКС**

Закон № 152-ФЗ: ЧТО НОВОГО В 2021 ГОДУ?



В марте 2021 г. вступили в силу поправки в Федеральный закон «О персональных данных», а в июле – новые правила контроля и надзора за соблюдением законодательства о персональных данных. Чтобы выполнить новые требования, участникам рынка в очередной раз придется приложить немало усилий.

Ольга Ермакова,
старший юрисконсульт и комплаенс-специалист,
Linxdatacenter

Рассказываем, что изменилось, как соблюдать и что будет, если пренебречь.

С 1 марта 2021 г. Федеральный закон № 152-ФЗ дополнился статьей 10.1, которая определяет особенности обработки персональных данных (ПДн), разрешенных субъектом данных для распространения. Нельзя сказать, что ст. 10.1 устанавливает принципиально новый подход к обработке данных, ранее не закрепленный в законе: и до марта 2021 г. 152-ФЗ не позволял третьим лицам бесконтрольно использовать персональные данные субъектов; для любой обработки требовалось соблюдение условий, перечисленных в законе, в том числе соответствие характера использования цели обработки. Вместе с тем в законе отсутствовали реальные механизмы контроля самого субъекта над распространением его данных. Теперь ситуация кардинально изменилась.

Во исполнение новой нормы Роскомнадзор издал Приказ от 24.02.2021 № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения», который вступил в силу 1 сентября 2021 г. Кроме того, 30 июня 2021 г. ведомство запустило онлайн-сервис, позволяющий оператору ПДн подготовить шаблон формы согласия и получить рекомендации по формированию согласия.

Загрузите обновления

Новые правила, по сути, ликвидировали понятие «общедоступные данные», заменив его новым – «персональные данные, разрешенные субъектом для распространения», и установили ряд требований к обработке указанных данных.

Если ранее обрабатывать данные, сделанные субъектом общедоступными, можно было без его согласия, то теперь, напротив, обработка данных, разрешенных субъектом для распространения, возможна лишь с его согласия. Иными словами, закон больше не придерживается

концепции «молчаливого согласия» субъекта на распространение его данных, более того, он устанавливает специальные требования к согласию на обработку, а именно:

- такое согласие должно быть получено отдельно от иных согласий;
- требования к согласию утверждает Роскомнадзор (см. упомянутый Приказ № 18);
- использование форм согласия на распространение данных, самостоятельно разработанных оператором ПДн, не допускается.

Не будем перегружать статью перечислением требований к согласию, ведь сейчас доступен сервис Роскомнадзора, который дает оператору ПДн возможность подготовить шаблон формы согласия, а также получить рекомендации по формированию такого согласия. Для заполнения формы потребуется учетная запись на портале госуслуг. Сформированная форма согласия приходит на указанную электронную почту в течение нескольких минут, рекомендации по формированию – в течение нескольких дней.

Тем не менее отметим три основных момента в работе с новой формой согласия:

1. Форма согласия потребует от оператора ПДн указать информационные ресурсы, посредством которых доступ к данным будет предоставляться неограниченному кругу лиц (адрес сайта в интернете).
2. Данные в согласии должны быть разделены на категории (общие, специальные, биометрические).
3. В рамках каждой категории ПДн должен быть сформирован перечень, по каждому пункту которого (отдельно фамилия, имя, отчество и т.д.) субъект выражает свое согласие или устанавливает запреты или условия обработки:
 - ▶ разрешение на распространение данных;
 - ▶ разрешение на распространение неограниченному кругу лиц;

- ▶ условия и запреты относительно распространения конкретных данных;
- ▶ дополнительные условия обработки указанных данных.

Несмотря на то что выполнение этих требований потребует от операторов ПДн немалых усилий, сам подход к выражению субъектом согласия, очевидно, повысит информированность последнего при предоставлении согласия и, кроме того, даст ему контроль над своими данными.

К получению согласия субъектов по утвержденной Роскомнадзором форме следует относиться ответственно: если в согласии на обработку ПДн, разрешенных их субъектом для распространения, отсутствует указанная в Приказе № 18 информация, то такие персональные данные должны обрабатываться оператором без передачи неограниченному кругу лиц и без возможности осуществления ими иных действий с персональными данными.

Кроме того, публикуя данные субъектов на своем веб-сайте, оператор теперь обязан опубликовать на этом сайте и информацию о запретах на обработку и передачу ПДн, а также условия их обработки и передачи неограниченному кругу лиц. Сделать это нужно в течение трех рабочих дней после получения согласия на обработку персональных данных, разрешенных субъектом для распространения.

Кто и как почувствует

Изменения отразятся в первую очередь на ИТ-секторе: операторах сайтов и цифровых сервисов, использующих ПДн (соцсети, пользовательские приложения). Также влияние новых требований испытают на себе все компании, собирающие и обрабатывающие большие объемы общедоступных данных: образовательные и медицинские учреждения, транспортные, телекоммуникационные и финансовые компании.

Цель понятна: ранее субъекты, делая свои ПДн общедоступными в определенных целях, сталкивались с ситуацией, когда их данные собирались третьими лицами и использовались в целях для субъекта нежелательных, а иногда и вовсе в противоправных. Изменения в законе позволяют уменьшить количество как непреднамеренных утечек, так и осознанных «сливов» ПДн.

Более строгие требования к оператору на этапе первичного сбора ПДн, а также повышение прозрачности и осведомленности участников рынка о правилах работы с данными, разрешенными субъектами для распространения, позволят вернуть субъектам контроль над своими данными и избежать негативных последствий, сопутствующих бесконтрольному движению данных, сделанных некогда общедоступными.

Кроме того, смеем надеяться, что нововведения умерят избыточную активность компаний при сборе данных: бизнес нередко превышает необходимый целесообразный минимум.

Санкции

Нарушения требований закона в области ПДн больше не «караются» предупреждением: регулятор сразу начинает с денежных взысканий, размер которых для некоторых видов нарушений увеличился вдвое или даже втрое.

За неправильно оформленное согласие должностное лицо в компании, курирующее вопросы данных, получит штраф 20–40 тыс. руб., а организация заплатит 30–150 тыс. руб. При повторном аналогичном нарушении сумма штрафа вырастет в два-три раза: 40–100 тыс. руб. для должностного лица и 300–500 тыс. руб. для компании.

Эти изменения лежат в русле тенденции к ужесточению наказаний, которая наблюдается последнее время в рассматриваемой сфере. В частности, в конце 2019 г. были установлены многомиллионные штрафы за неисполнение требований по локализации баз данных с ПДн граждан РФ на территории России: штраф за первое нарушение для юрлиц составляет теперь 1–6 млн руб., за повторное – 6–18 млн руб.

А судьи кто?

Прослеживается также тенденция к усилению контроля за обработкой ПДн: 1 июля 2021 г. вступило в силу Положение о федеральном государственном контроле (надзоре) за обработкой персональных данных (утверждено Постановлением Правительства РФ от 29.06.2021 № 1046). Новый документ отменил действовавшие с 2019 г. Правила организации и осуществления государственного контроля и надзора за обработкой персональных данных (утверждены Постановлением Правительства РФ от 13.02.2019 № 146). Напомним, административный регламент, на смену которому пришло Постановление № 146, действовал почти восемь лет, а само оно было в работе чуть менее полутора лет. Очевидно, что действия при обработке ПДн находятся сегодня в фокусе внимания регулятора, и можно с уверенностью утверждать, что тенденция сохранится.

Согласно новым правилам, при осуществлении государственного контроля за обработкой ПДн применяется система оценки и управления рисками, а само Постановление № 1046 содержит критерии отнесения объектов контроля к той или иной категории риска. Постановление определяет пять категорий риска: высокий, значительный, средний, умеренный и низкий. Это соответствует подходу к оценке и управлению рисками причинения вреда охраняемым зако-

ном ценностям, закрепленному в Федеральном законе от 31.07.2020 № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации».

Периодичность плановых проверок теперь связана с категорией риска: для компаний, отнесенных к категории высокого риска, проверка будет проводиться один раз в два года, значительного риска – раз в три года, среднего риска – раз в четыре года, умеренного риска – раз в шесть лет. Лица, деятельность которых в связи с обработкой ПДн отнесена к категории низкого риска, плановым проверкам не подвергаются.

Категории риска определяются, в частности, категориями данных, обрабатываемых операторами: компания, обрабатывающая специальные или биометрические персональные данные, будет отнесена к высокой категории риска. Информацию регулятор почерпнет в том числе из уведомлений, поданных операторами в соответствии со ст. 22 закона № 152-ФЗ.

Помимо категоризации рисков государственный контроль и надзор в этой области дополнился такими механизмами, как объявление предостережения о недопустимости нарушения обязательных требований, консультирование и профилактический визит.

Собственно проверки теперь могут проходить в трех формах: инспекционный визит, документарная проверка и выездная проверка. Сроки уведомления о проверках едины для всех форм государственного контроля и надзора и указаны в упомянутом законе № 248-ФЗ.

Выводы и выходы

Несмотря на тенденцию к увеличению штрафов, в России за нарушения в сфере ПДн пока наказывают несопоставимо мягче, чем в ЕС или США. Так, немецкая компания группы H&M, известного производителя одежды и товаров для дома, недавно была оштрафована на 35,3 млн евро за нарушения при обработке персональных данных работников.

Вместе с тем пристальное внимание российских властей к вопросам обработки данных очевидно. Чтобы не оказаться в одном списке с оштрафованными организациями, нарушившими правила работы с ПДн, необходимо предпринять ряд шагов.

Во-первых, провести тщательный аудит бизнес-процессов, в которых задействуются персональные данные. По результатам аудита нужно принять организационные, правовые и технические меры для защиты данных, включая проектирование систем безопасности в ИТ-ресурсах компании, распределение ролей сотрудников и т.д.

Во-вторых, необходимо реформировать корпоративную культуру – в частности, выработать привычку заниматься вопросами безопасности данных постоянно. **ИКС**



Энергия интеллекта

Ведущее аналитическое агентство России и СНГ в сфере телекоммуникаций, ИТ и медиа

- Аналитика
- Стратегии
- Бизнес-планирование
- Информационно-аналитическая поддержка
- Потребительские опросы в B2C и B2B сегментах



Лондон



Киев



Москва



Алматы

ИТ

Телеком

Медиа

Контент и сервисы

Системная интеграция

Голосовые услуги

Платное ТВ

Навигация и LBS

Дата-центры

ШПД

Мобильное видео

M2M

Облачные сервисы

Мобильный интернет

Игры

NFC

ИТ инфраструктура

VAS

Интернет-порталы

E-commerce

Офисная техника

Межоператорские услуги

Видео-контент

Теле-медицина

Чек-лист безопасности облачных сервисов



Александр Ветколь,
ведущий системный инженер,
Varonis

Как сделать облачную инфраструктуру не менее защищенной, чем классическую инфраструктуру on-premise? Прежде чем переходить к выбору конкретных инструментов, есть смысл определить основные направления работы по защите данных в мультиоблачных средах.

Процесс повсеместной «облачной трансформации» все ускоряется. Этому способствуют и растущая доля сотрудников, работающих удаленно, и тенденция к созданию полностью распределенных коллективов, которые могут иметь глобальный охват. В таких сценариях инфраструктура on-premise по финансовым показателям и трудозатратам на подготовку вчистую проигрывает распределенным облачным сервисам, уже развернутым и одинаково доступным из любой точки планеты. Еще один драйвер – оптимизация расходов. Возможность платить только за реально потребленные ресурсы делает облачные сервисы гораздо привлекательнее собственных дата-центров, операционные расходы на которые почти постоянны, даже если большая часть ресурсов простаивает.

Однако может ли облачная инфраструктура быть не менее защищенной, чем дата-центр на площадке компании? По данным исследования «Лаборатории Касперского», 26% российских компаний выражают свое беспокойство по этому поводу. В мире в целом эта цифра еще выше (что странно, обычно именно наши специалисты более полно осознают риски, на которые они никак повлиять не могут) – 33% сомневающихся хотя бы в сравнимом уровне защищенности.

Облачные угрозы

С ростом популярности облаков неизбежно растет и количество связанных с ними инцидентов информационной безопасности. И если, по различным оценкам, по доказанной вине провайдеров облачных услуг происходит около 11% подобных событий, то более 30% вызваны человеческим фактором – сотрудники компаний становятся жертвами приемов социальной инженерии. Если говорить о подтвержденных утечках корпоративных данных из облака, то, по данным упомянутого исследования «Лаборатории Касперского», 90%

подобных случаев произошли из-за ошибок сотрудников.

При этом с ростом потребления облачных услуг усложняются сценарии их использования. Инфраструктуры все чаще становятся гибридными и мультиоблачными. Это, в свою очередь, усложняет и ландшафт угроз, что требует приобретения дополнительных, зачастую узконаправленных, инструментов обеспечения информационной безопасности. При планировании сокращения расходов после переноса бизнес-процессов в облака это обстоятельство надо учитывать.

Взломы последних лет дают повод задуматься. В 2015 г. крупная утечка учетных записей пользователей произошла в Slack. В течение четырех дней хакеры имели доступ к инфраструктуре провайдера сервиса для совместной работы. Об этом давнем инциденте снова заговорили в 2019 г., когда оказалось, что многие из украденных «учеток» до сих пор активны и используют те же связки «логин – пароль». Компании тогда пришлось принудительно сбросить пароли примерно 1% своей аудитории.

Не менее примечательные инциденты имели место и с Zoom – сервисом для групповых видеоконференций, популярность которого взлетела до небес на фоне пандемии коронавируса. В апреле 2020 г. тысячи учетных записей пользователей этой платформы были опубликованы на одном из хакерских форумов. Нередко записи частных видеоконференций удавалось обнаружить на YouTube.

Какие ИБ-риски характерны для облаков

Каждый облачный сервис использует собственные механизмы предоставления прав доступа, свои типы данных и форматы журналов активности. Из-за отсутствия единых принципов контроля данных и обеспечения их доступ-

ности такие сервисы могут сделать компанию уязвимой перед внешними или инсайдерскими атаками. Для того чтобы эти риски имели шанс воплотиться в конкретных инцидентах, компании достаточно совершить одну из четырех основных ошибок:

- не наладить систему контроля выдачи прав доступа. Это рано или поздно может привести к тому, что данные окажутся в распоряжении, например, уволенного сотрудника;
- разрешить доступ к корпоративным данным из личных учетных записей и не установить ограничения на географическое местоположение пользователей. Личные учетные записи легко могут быть скомпрометированы, а подключение пользователя из нетипичного для него региона без предварительно согласованного разрешения почти всегда свидетельствует о том, что учетная запись украдена;
- не вести полноценного журналирования активностей, связанных с доступом к данным. Отсутствие такой информации усложнит расследование инцидентов и не позволит усилить периметр безопасности на необходимых направлениях. Отметим, что в большинстве популярных облачных сервисов встроенных инструментов наблюдения за активностью пользователей нет;
- не отслеживать случаи нестандартного поведения пользователей. Это может привести к тому, что администратор, например, не заметит вовремя массовое удаление файлов или их отправку за пределы защищаемой инфраструктуры.

Конечно, использование многофакторной аутентификации (Multi-Factor Authentication, MFA) и брокеров доступа к средам (Cloud Access Security Broker, CASB) может существенно снизить риски, но не устранить их полностью.

Чек-лист облачной безопасности

Перед тем, как переходить к практической стороне защиты данных в мультиоблачных средах и выбору конкретных инструментов, есть смысл обозначить основные направления этой работы:

1. Для того чтобы уменьшить площадь потенциальной атаки на облачный сервис, надо следить за тем, чтобы каждый из сотрудников (возможно, на базе ролевой модели, что упростит задачу) получал лишь минимально необходимый набор прав на операции с данными. Такую работу нужно вести непрерывно – недостаточно однократно определить перечень прав при подключении работника к сервисам. Этот перечень должен постоянно пересматриваться. Если права сотрудника стали избыточными для выполнения конкретной работы (например, изменились его обязанности и, как следствие, его роль), они должны быть не-

медленно отозваны. Часто те работники, которые по какой-либо причине получили избыточные привилегии, начинают использовать их для целей, не связанных с рабочими процессами. Это повышает риск инсайдерской атаки, а также возможный ущерб при краже такого аккаунта.

2. Необходимо постоянно отслеживать активность пользователей на предмет аномальных действий или нарушений принятых в компании правил работы. Отход от стандартной модели поведения укажет на возможную компрометацию учетной записи или же на недобрые намерения самого пользователя.

3. Отслеживать надо не только активность аккаунтов, но и ее отсутствие. Если аккаунт, присвоенный сотруднику или какому-либо бизнес-процессу, длительное время простаивает, он должен быть отключен. Иначе подобный «призрак» в системе легко может стать входными воротами для хакерской атаки.

4. Необходимо регулярно передавать отчеты о проверке прав руководителям бизнес-подразделений. Хорошо зная ситуацию в своих департаментах, они без труда определяют, для каких аккаунтов и токенов приложений права должны быть изменены или отозваны.

5. Следует подобрать инструменты безопасности таким образом, чтобы они были способны контролировать угрозы, охватывающие несколько облачных сервисов. Зачастую средства ИБ, которыми облачные платформы оснащены по умолчанию, видят только ту часть атаки, которая приходится на их инфраструктуру. Такой обзор не всегда будет полным. На рынке есть продукты, осуществляющие унифицированный контроль облачных сред и приложений с различной функциональностью.

6. Нужно регулярно проводить аудит настроек общего доступа. Это поможет не допустить случайной или преднамеренной утечки данных просто в силу того, что конфиденциальный файл оказался в папке с излишне широкими правами.

7. Необходимо сделать процесс отключения учетных записей и отзыва прав доступа обязательной частью процесса увольнения сотрудников или прекращения работы с подрядчиками. Это даст возможность избежать ситуации, когда часть облачных сервисов остается вне вашего контроля. Облегчить эту задачу помогут решения для управления сущностями и доступом к ним (Identity and Access Management, IAM), которые позволяют гибко работать с учетными записями сотрудников и выданными им правами доступа при изменениях их статуса, в том числе при увольнении или переводе на другую должность. ИКС



СИБП с возможностью «горячей» замены

Компания Schneider Electric анонсировала расширение функциональности трехфазных ИБП Galaxy VS: теперь доступны модификации мощностью 20–150 кВт (400 В), а модели с внешними батареями оснащены поддержкой Live Swap.

Live Swap – это технология, обеспечивающая защиту от поражения электрическим током при прикосновении в процессе замены или добавления силовых модулей в работающий и подключенный к сети ИБП. Live Swap дает возможность осуществить безопасную «горячую» замену модулей без выключения ИБП и нагрузки, а также без перевода техники в режим механического байпаса. Функциональность и надежность решения подтверждены независимыми тестами лаборатории UL.

Помимо поддержки технологии Live Swap новые функции Galaxy

VS включают в себя удобный подсчет сэкономленной электроэнергии в режиме EConversion и подключение по схеме ИТ (без нейтрали).

Поддержка Live Swap опциональна и может быть приобретена вместе с ИБП или установлена на уже функционирующем устройстве. Решение доступно в семействе ИБП Galaxy VS только для моделей без встроенных батарей, однако позже поддержка этой технологии будет реализована и в остальных продуктах семейства Galaxy VS.

www.se.com/ru/ru

Модульные ИБП для дата-центров

Компания «Парус электро» выпускает модульные ИБП серии СИП380А МД, построенные на модулях 50 кВт. Резервирование силовых модулей и блоков управления обеспечивает надежность, соответствующую требованиям к ЦОДам и критической информационной инфраструктуре, а возможность их «горячей» замены без отключения нагрузки – максимальную ремонтпригодность и простое наращивание мощности системы.

Модельный ряд кабинетов ИБП охватывает мощности от 150 до 1000 кВА. За счет параллельного включения до четырех систем возможно увеличение мощности до 4 МВт или резервирование на уровне систем бесперебойного питания.

Применение в ИБП СИП380А МД новых схемотехнических решений на основе трехуровневого инвертора увеличило коэффициент выходной мощности до 1,0 и позволило подключать больше оборудования с повышенной активной мощностью. Плотность мощности более 300 кВт на 19-дюймовый шкаф упрощает размещение и подключение ИБП.



Сокращение эксплуатационных расходов на электроэнергию достигается благодаря КПД более 96%. Высокая эффективность преобразования энергии не только уменьшает потери, но и понижает затраты на отвод избыточного тепла.

Большой цветной сенсорный экран с интуитивно понятным интерфейсом облегчает контроль и настройку работы ИБП. Мониторинг ИБП обеспечивается через популярные коммуникационные протоколы Modbus или SNMP, вплоть до защищенной версии 3, что упрощает интеграцию ИБП в корпоративные системы управления.

www.parus-electro.ru

Решение для обеспечения бесперебойного электропитания

Компания SME представляет серию решений для обеспечения бесперебойного электропитания – SME ArtModular Energy.

В этих решениях используются готовые энергомодули на основе источников электропитания ведущих мировых производителей, что гарантирует непрерывную работу оборудования. В частности, применение солнечных батарей поможет уменьшить углеродные выбросы.

Мощность ИБП одного модуля – до 10 кВА с возможностью масштабирования до 12 МВА. Время автономной работы варьируется от 5 до 50 мин с возможностью увеличения при использовании батарей-

ных контейнеров расширения. Все решения полностью укомплектованы системами пожаротушения, кондиционирования, удаленного мониторинга, видеонаблюдения и необходимыми электрическими системами.

Опционально возможно использование литий-ионных источников питания и систем гибридного электроснабжения, где обе системы питания дополняют друг друга, работая в ротационном режиме.

www.sme-russia.ru



Облачное решение для оценки эффективности сетей радиодоступа 5G

Компания Keysight Technologies анонсировала выпуск пакета ПО Nemo 5G RAN Analytics – полностью автоматизированного облачного решения для ускоренной обработки данных, подготовки отчетов и дистанционного контроля сетей радиодоступа (RAN) пятого поколения.

В основе ПО Keysight Nemo 5G RAN Analytics лежит централизованная сетевая платформа управления данными, предназначенная для анализа и подготовки отчетов на уровне предприятия. Этот пакет ПО позволит операторам, сервисным подрядчикам и производителям сетевого оборудования ускорить процедуры приемки, оптимизации, тестирования и устранения неполадок в развертываемых сетях. Nemo 5G RAN Analytics применяет инструменты анализа данных, встроенные элементы искусственного интеллекта и

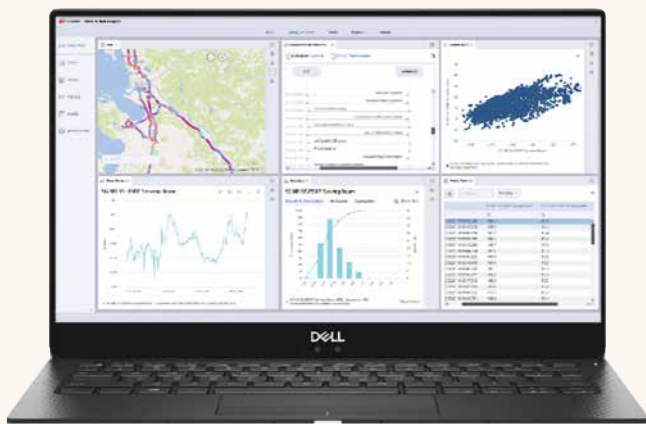
машинного обучения в сочетании с интуитивно понятным пользовательским интерфейсом для эффективной обработки больших массивов данных в работающих сетях 5G.

Nemo 5G RAN Analytics помогает автоматизировать ряд процедур, требующих взаимодействия между организациями, в том числе:

- анализ радиочастот, оценку пропускной способности каналов и характеристик голосовой связи;
- выявление неполадок в сетях и анализ их коренных причин;
- дистанционный контроль сетей в режиме, близком к режиму реального времени;
- тестирование эффективности работы устройств и сетей мобильной связи;
- создание, контроль и распространение отчетов и таблиц с возможностью индивидуальной настройки для каждого пользователя;
- анализ эффективности приложений для трансляции видео в интернете, таких как YouTube, Facebook, WhatsApp и Twitter.

Nemo 5G RAN Analytics поставляется на условиях «программное обеспечение как услуга» (SaaS) и полностью интегрируется с другими решениями Keysight Nemo.

www.keysight.com



ДАТАПРО

Тел.: (495) 800-8000

E-mail: info@datapro.ru

www.datapro.ru 1-я обл.

ИНФОСИСТЕМЫ ДЖЕТ

Тел.: (495) 411-7601

Факс: (495) 411-7602

E-mail: info@jet.su

www.jet.su с. 60–61

СВОБОДНЫЕ ТЕХНОЛОГИИ ИНЖИНИРИНГ

Тел.: (495) 120-2866

E-mail: info@sv-tech.ru

www.sv-tech.ru 4-я обл.

EMILINK GROUP

Тел.: (800) 777-1300

E-mail: info@emilink.ru

www.emilink.ru с. 68–69

RITTAL

Тел.: (495) 775-0230

Факс: (495) 775-0239

E-mail: info@rittal.ru

www.rittal.ru с. 43, 44–45

SCHNEIDER ELECTRIC

Тел.: (495) 777-9990

Факс: (495) 777-9992

www.schneider-electric.ru с. 54–55

Указатель фирм и организаций

3Com 66	Mail.ru Cloud Solutions 80	Банк России 85	«Новые облачные
3data 10, 14, 38, 53	METAENERGY 14	«Веза» 14	технологии» 21
ABB 36, 38, 39	Microsoft 19, 21, 42, 80, 85, 88	ВТБ 7, 11	«Новые Технологии» 13
AceOn 53	Mitsubishi Electric 14, 41	ВЭБ.РФ 11	НТЦ ИТ РОСА 21, 78
Alibaba Cloud 80	Molex 66	Департамент информационных	«ОМП-Инжиниринг» 13, 14
Astra Linux 78	Oracle 7	технологий Москвы 7, 31	«Онланта» 79
AWS 19, 80	Perkins 14	ДКС 10, 13, 15	«Оптическое волоконные
Axis 82	Postgres Professional 6	ЕАЭС 5	системы» 69
BellSoft 6, 7	QazCloud 4, 11	«ИКС-Медиа» 4, 8, 13, 35	«Парус электро» 14, 94
C3 Solutions 13, 15	Red Hat 6, 7, 20	Институт статистических	«ПламСпейс» 32
Centron 59	Rittal 9, 40, 41, 44, 45	исследований и экономики	«ПНК Групп» 39, 40
Citrix 9	RS2E 53	знаний при ВШЭ 75	ГК «Пожтехника» 14
Corning 69	Schneider Electric 5, 9, 14, 36,	«Казахтелеком» 4	«Промобит» 17
Cummins 14 37, 54, 55, 60, 94	«Казтелпорт» 4, 5	«ПрофАйтиКул» 56
DataLine 87, 88	SDMO 60	Корпорация развития Дальнего	ПФР 29
DataPro 8, 9, 10, 36	Selectel 8	Востока и Арктики 11	«Росатом» 30
DC development 39, 40	Slack 92	«КОСТРОМАКАБЕЛЬ» 68	Роскомнадзор 87, 89, 90
Delta Electronics 14, 39	SME 37, 38, 95	КРОК 62	Российский национальный
Duo Security 86	Softline 76, 78	«Лаборатория	коммерческий банк 6
Eaton 42	Stamford 14	Касперского» 92	Росстат 29
ГК EMILINK 68, 69	Stulz 60	ГК ЛАНИТ 11, 16, 19, 79	«Ростелеком» 11
Faradion Limited 53	Thales 87	«ЛАНИТ-Интеграция» 16, 19	«Ростелеком-ЦОД» 8, 10, 11
Gigabyte 11	Tiamat 53	МГУ 53	«Р-Платформа» 78
Google 7, 19, 85, 86	Tionix 78	Минздрав России 26	«Русатом инфраструктурные
GreenBushDC 8	Tutu.ru 28	Минпромторг России 21	решения» 30
HiNa 53	Uptime Institute 46, 48,	Минцифры России 6, 10,	«Рейдикс» 18
H&M 91 49, 50, 51, 53 13, 22	Сбер 87
Hosser Telecom Solutions 38, 60	Veeam Software 10	Мостуризм 30	«Свободные Технологии
Huawei 4, 8, 40	Vertiv 36, 60	МТС 8	Инжиниринг» 35, 36
IBM 6, 7, 20	«VK Цифровые Технологии» 11	МТУСИ 64	«Скала-Р» 78
ГК IEK 13	Yadro 16	«Надежный Цифровой Сервис	«Сколково» 32
iKS-Consulting 4, 5, 8, 23,	Zoom 92	Данных» 11	ГК «Темпесто» 38
. 28, 29, 31, 88	ZutaCore 40, 41	«Нанософт» 65	«Транстелеком» 4
INNIO Jenbacher 42	«Авантаж» 8	«Национальные информацион-	«Узбектелеком» 4
Intel 41	«АКАДО Телеком» 38	ные технологии» 4	«Узинформ» 4
ITK 13, 15	АНО «Координационный совет	Национальный институт	Университет Инха 4
IXcelerate 8, 9, 10, 15	по ЦОДам и облачным	стандартов	ФБР 85
Juniper 5	технологиям» 10, 11, 22	и технологий США 86	ФСС России 29
Kehua Tech 39	АНО «Центр компетенций	Национальный центр научных	ЦРИ «Импульс» 14
Key Point 11	по импортозамещению	исследований Франции 53	«ЭлНетМед» 26
Keysight Technologies 95	в сфере ИКТ» 7	«Нетрика Медицина» 26, 72	«Яндекс» 7, 11, 30
Leroy Somer 14	«Аэродиск» 17, 70	«Новые коммуникационные	«Яндекс Облако» 80
Linxdcenter 89	«Базальт СПО» 21	технологии» 21	

Учредители журнала «ИнформКурьер-Связь»:

ООО «ИКС-Медиа»:

105066, Москва
ул. Новорязанская, д. 31/7, корп. 14;
тел.: (495) 150-6424

МНТОРЭС им. А.С. Попова:

107031, Москва, ул. Рождественка,
д. 6/9/20, стр. 1;
тел.: (495) 921-1616.

11-я международная конференция

CLOUD & DIGITAL
TRANSFORMATION



ПЕРЕОСМЫСЛИ БИЗНЕС

март 2022

Цифровая трансформация – ключ к «выживанию» и устойчивому развитию отдельных компаний и экономики в целом. А наличие современных ИТ-сервисов, реализуемых по облачной модели, – необходимое условие такой трансформации. На конференции CLOUD & DIGITAL TRANSFORMATION – самая полная информация о технологиях и сервисах, а также обмен опытом использования облаков в процессе преобразования бизнеса.

Основные темы



Отраслевой опыт цифровой трансформации



Мультиклауд: возможности и риски



Импортозамещенные облака – миф или реальность



Как дотянуться до облака: сетевая связность

Реклама

ОРГАНИЗАТОР



ПРИ ПОДДЕРЖКЕ



Минцифры
России



КООРДИНАЦИОННЫЙ СОВЕТ
ПО ЦОДам И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ
Автономная некоммерческая организация

16+

ЗАРЕГИСТРИРОВАВШИМСЯ БУДЕТ ДОСТУПНА
ВИДЕОЗАПИСЬ НА САЙТЕ КОНФЕРЕНЦИИ



cloud-digital.ru



СВОБОДНЫЕ
ТЕХНОЛОГИИ
ИНЖИНИРИНГ

ПРОСТЫЕ РЕШЕНИЯ СЛОЖНЫХ ЗАДАЧ

ПРОЕКТИРОВАНИЕ И СТРОИТЕЛЬСТВО ДАТА-ЦЕНТРОВ

Россия, 127055, Москва,
Бутырский вал, д. 68/70, стр. 2
+7 (495) 120-28-66
info@sv-tech.ru
www.sv-tech.ru

