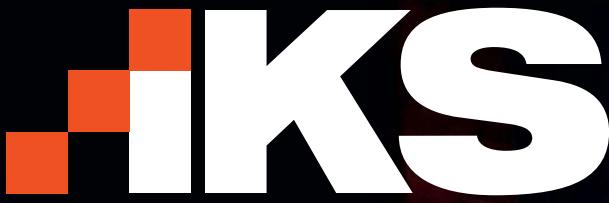


Газовая генерация
для ЦОДов
стр. 32

Гонка
суперкомпьютеров
стр. 42

Возрождение
«голого металла»
стр. 65

Оценка рисков
безопасности
стр. 74



ИнформКурьер-Связь

Издаётся с мая 1992 г.

Тема номера

**ПРОБЛЕМЫ
ВЫБОРА СИСТЕМЫ
ВИРТУАЛИЗАЦИИ**

www.iksmedia.ru

№1 ■ 2025



ЦОДы – дело жизни

МЕРОПРИЯТИЯ ИКС-МЕДИА

2025

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

Реклама/16+

География:

Москва
Санкт-Петербург
Екатеринбург
Новосибирск
Ташкент
Алматы



подробнее
на сайте iksmedia.ru

IKS



ХАП ВОКРУГ ЦОДов

В прогнозах мировых аналитических агентств все чаще стал встречаться термин «ИИ-ЦОД» (AI DC). Но четкого определения, что же такое ЦОД для искусственного интеллекта, в чем его основные отличия от обычного ЦОДа, я нигде не нашел. В основном хайп и маркетинг.

В привязке к ИИ все говорят о стремительном росте плотности мощности. Так, в дорожной карте Vertiv, гармонизированной с планами Nvidia, значится выход к 2029 г. на уровень 1 МВт на стойку – миллион (!) ватт на стойку.

Высокоагруженные стойки (25+ кВт) – это, скорее всего, гибридное охлаждение: воздушное + прямое жидкостное контактное. Однако не все сводится к охлаждению. При использовании традиционных технических решений уже 32 кВт на стойку приведут к тому, что площадь, занимаемая в ЦОДе системами электропитания, вдвое превысит площадь машзалов (оценка Huawei). Чтобы удержать это соотношение на уровне хотя бы 1:1, нужно новое поколение компактных систем электропитания.

GPU-системы для ИИ – это еще и специфическая нагрузка, характеризующаяся кратковременными (примерно 50 мс) пиками потребления до 150% среднего. Ваши ИБП готовы к такому режиму или будут «сваливаться» на байпас? Наверное, для компенсации этих пиков традиционные ИБП с аккумуляторами не самое подходящее решение. Лучше подойдут, например, суперконденсаторы. Но и здесь может наступить время гибридов: суперконденсаторы (для компенсации коротких пиков) будут сочетаться с традиционными аккумуляторами (для обеспечения длительного времени автономии).

Вернемся к плотности мощности. Практики с большим опытом в области цдостроения в качестве максимальной мощности на стойку через пять лет называют 100–200 кВт. Средняя же будет на порядок ниже, 12–15 кВт. Просто потому, что GPU-фермы для обучения ИИ-моделей нужны далеко не всем, проще и выгоднее получать соответствующие ресурсы по сервисной модели у гиперскейлеров или крупных провайдеров.

ЦОДы, конечно, будут другими. И мой прогноз: до 1 МВт на стойку дело не дойдет. Конец этой безумной гонке положит практическая целесообразность или новое поколение ИТ-систем, например, на базе фотонных процессоров. Но пока отрасль только нащупывает альтернативные решения, обеспечивающие более эффективное использование мощностей, площадей и других ресурсов.

Александр Барсков
Главный редактор

1 Колонка редактора**[ИКС-Панорама]****4**

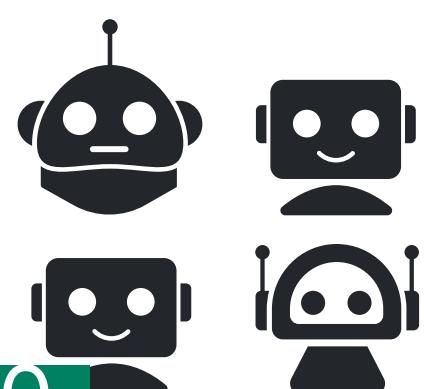
В будущее под всеми парусами

6Отрасль ЦОДов: проблемы
роста и региональная
специфика**9**ЦОДы в Узбекистане: как снять
барьеры**10**

Дайджест отрасли ЦОДов

[Экономика и бизнес]**12**С. ВЫШЕМИРСКИЙ. ЦОДы
в условиях дефицита
электроэнергии**16**А. МАРТЫНЮК. ЦОДы – дело
жизни**20**М. МИЛКОВ, А. САЛИН.
Цифровые ассистенты
и прогнозные модели:
ИТ-тренды в промышленности
2025 года**22**Т. НУГМАНОВ. ЦОД как сервис –
услуга стала доступнее

Тема номера

**ПРОБЛЕМЫ
ВЫБОРА СИСТЕМЫ
ВИРТУАЛИЗАЦИИ****6****12****20**



54

[Инфраструктура]

24

А. СЕМЕНОВ, Н. КУДРЯВЦЕВ.
Данные и питание по одному кабелю

30

А. ОВЧИННИКОВ. VSP Global: от проектировщика к ЦОД-девелоперу

32

М. КОТЛЯРОВ, В. ЧУМАЧЕНКО, С. ПАСКЕВИЧ. Построение системы энергоснабжения крупных ЦОДов на базе газовой генерации

37

И. БОРНЯКОВ. Почему будущее СХД за IP-протоколами

40

ABSolite: бесперебойное электропитание от надежного поставщика

42

Н. НОСОВ. Гонка суперкомпьютеров: обойти на повороте

46

Г. КАРУЛИН. Натриевые АКБ: на старт, внимание, марш!

48

Е. ШЛЫК. Пожарная безопасность ЦОДа: не автоматикой единой

52

В. ШЕПЕЛЕВ. Envicool: слагаемые успеха

[Сервисы и приложения]

54

Н. НОСОВ. Брачные игры павлинов, или Проблемы выбора системы виртуализации

61

И. БЕДЕРДИНОВ, Ф. ПОПКО. GPUaaS: что предлагают российские провайдеры

65

А. САЛОВ. Облачные итоги – 2024. Возрождение «голого металла»

[Безопасность]

68

Н. НОСОВ. Карты таро и другие способы оценки рынка информационной безопасности

74

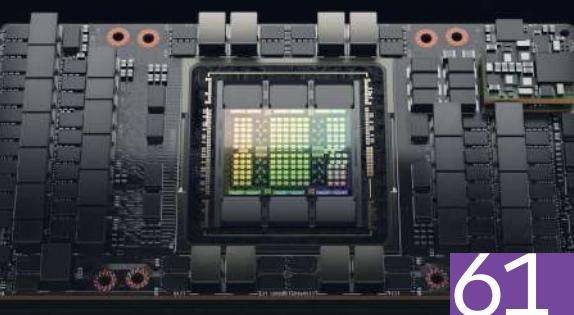
Д. КОСТРОВ. Оценка рисков информационной безопасности: сколько вешать в граммах

78

Содержание журнала «ИКС» в 2024 г.



24



61



68

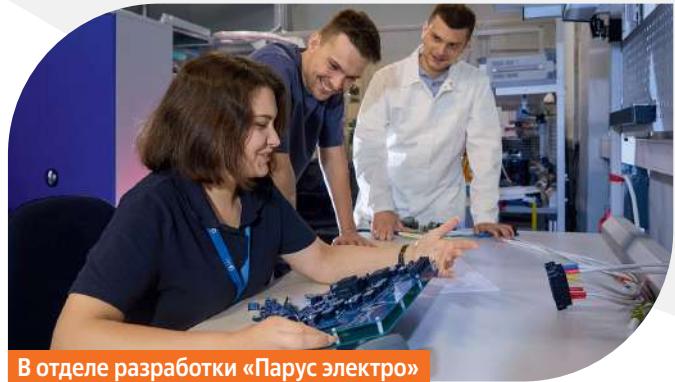
В будущее под всеми парусами



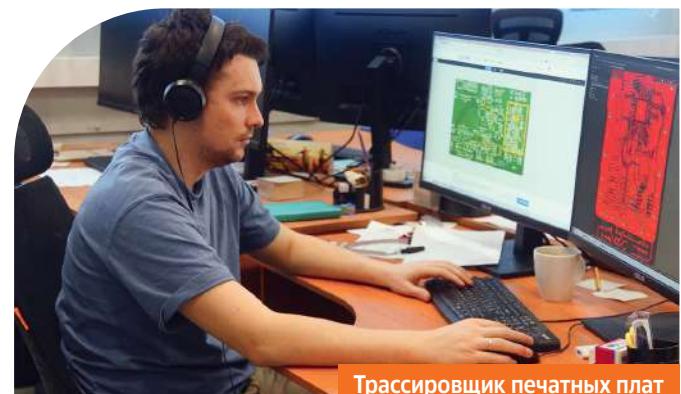
«Когда дует ветер перемен, ставь не стены, а паруса», – гласит восточная мудрость. Ветер перемен подул с такой силой, что многим стало непонятно, что делать дальше. Но это не относится к компании «Парус электро», которая и до «перемены ветра» двигалась в направлении отечественного производства, а теперь просто расправила паруса.

Более того, компания не только совершенствует традиционную для себя продукцию – системы бесперебойного питания, но, опираясь на свой опыт работы с силовой электроникой, осваивает ниши, освободившиеся после ухода западных компаний: зарядные станции для электромобилей и преобразовательную технику для возобновляемых источников энергии. Всё в соответствии с «зеленой повесткой»: снижаем загрязнение атмосферы – спасаем мир.

Не зря продукция «Парус электро» была представлена на форуме-фестивале «Территория будущего. Москва-2030». Действительно, предлагаемые компанией технологии смотрятся как картинки из будущего.



В отделе разработки «Парус электро»



Трассировщик печатных плат



Устройство для имитации серверной нагрузки

Создание нового изделия начинается в отделе разработки, в штат которого входят инженеры, программисты, электронщики, тестировщики и схемотехники. Разработанный продукт реализуется в виде опытных образцов.

В отдельной комнате производится трассировка печатных плат. Для ИБП в основном используются четырехслойные платы, хотя для сложной электроники здесь могут разрабатывать платы и в 12 слоев.

Электроника на печатную плату монтируется, как правило, тоже на заводе «Парус электро», в цехе, где в условиях стерильности работает аппаратура автоматической сборки.

Готовые опытные образцы возвращаются в отдел разработки, где их тщательно тестируют в разных режимах работы, в том числе на специально оборудованном стенде, имитирующем нагрузку серверов разной мощности.

Отдельный цех занимается обработкой поступающих из других подразделений завода и от внешних подрядчиков комплектующих. Подготавливаются проводные системы и кабельные сборки. В цехе металлообработки режется и гнется металл для корпусов, стоек и деталей конструкций.



Все комплектующие тщательно тестируются. Окончательная сборка производится в монтажном цехе, затем проверяется работа устройства в целом.

В числе новых наукоемких решений силовой преобразовательной техники – инверторы для солнечных электростанций. Они с минимальными потерями преобразуют постоянный ток от солнечных панелей в переменный ток промышленной электросети. Кроме того, сетевые инверторы используются для подключения к электросети и могут подавать в нее избыточную энергию.

Под заказ компания собирает электрозарядные станции для электромобилей. Модели отличаются высокой мощностью и обеспечивают быструю зарядку.

Приоритетное направление для компании по-прежнему – центры обработки данных. Для них «Парус электро» выпускает однофазные и трехфазные ИБП, делая упор на легко масштабируемые и отказоустойчивые модульные устройства. Для крупных data-центров есть решения со 100-киловаттными силовыми модулями с уникальными на рынке показателями плотности мощности.



На «Карте вендоров решений для ЦОД», которую готовит iKS-Consulting, «Парус электро» уверенно занимает первое место в категории ИБП. Эту лидирующую позицию можно считать отражением доверия крупных data-центров к продукции компании. «Парус электро» – настоящее российское производство, несмотря на все вызовы, уверенно прокладывающее путь в будущее.



парус
электро

parus-electro.ru

Отрасль ЦОДов: проблемы роста и региональная специфика



6-я конференция «ЦОД: модели, сервисы, инфраструктура», организованная «ИКС-Медиа» в конце ноября в Екатеринбурге и собравшая более 350 делегатов, по традиции стала местом подведения предварительных итогов развития рынка ЦОДов в 2024 г. и обсуждения его основных тенденций.

В 2024 г. число стойко-мест в российских коммерческих ЦОДах, согласно предварительным данным iKS-Consulting, увеличилось на 17% и достигло 82,4 тыс. Такие объекты по-прежнему в основном сконцентрированы в Москве – на нее приходится почти 76% соответствующего рынка. Столица опережает другие регионы и по темпам роста: в 2018–2024 гг. среднегодовой темп увеличения числа стойко-мест в коммерческих ЦОДах в Москве составил 14,5%, в Санкт-Петербурге – 7,4%, в других регионах – 11,1%.

В Екатеринбурге аналитики iKS-Consulting насчитали 10 коммерческих ЦОДов (см. таблицу). По этому показателю столица Урала находится на третьем месте в России. Правда,

по числу стойко-мест (613) – только на пятом, уступая еще Казани (1415) и Новосибирску (1034). Однако уже в следующем году стойко-мест в Екатеринбурге может стать в 2,5 раза больше: «РТК-ЦОД» намеревается серьезно расширить свой

Число коммерческих ЦОДов и стойко-мест в них в крупных городах России

действующий data-центр, а ГК Key Point планирует запустить первую очередь нового ЦОДа.

Названные две компании, наряду с «Росатомом», образуют тройку лидеров как по числу стойко-мест в региональных коммерческих ЦОДах, так и по темпам роста этого показателя в 2024 г. По плану у «РТК-ЦОД» этот рост составит 38% (+1052 стойко-места в data-центрах Удомли и Екатеринбурга), у «Росатома» – 129% (+1000 стойко-мест, ЦОД в Иннополисе), у ГК Key Point – 200% (+880 стойко-мест во Владивостоке и Новосибирске).

Город	ЦОДы	Стойки 2024п	Стойки 2025п
Москва	94	62 538	70 758
Санкт-Петербург	28	7 670	9 693
Екатеринбург	10	613	2 093
Новосибирск	7	1 034	1 778
Самара	4	490	490
Казань	4	1 415	1 415

Источник: iKS-Consulting

Все приведенные выше данные относятся к сегменту коммерческих ЦОДов, которые в основном и отслеживают аналитики. Однако, по оценке того же агентства iKS-Consulting, в России только около 18% стойко-мест приходится на коммерческие ЦОДы, остальные установлены в корпоративных (в западных странах это соотношение, по сведениям Uptime Institute, примерно 50 на 50). В таких промышленных регионах, как Урал, доля стоек в коммерческих ЦОДах, по всей видимости, еще ниже.

Специфика используемых информационных систем, повышенные требования к безопасности, а также наличие свободных площадей и энергетических ресурсов (особенно на крупных площадках) делают создание и развитие собственных ЦОДов более привлекательным для промышленных предприятий. И в ближайшее время, по мнению Олега Сидорова, директора технического департамента УЦСБ, сегмент корпоративных ЦОДов на Урале будет расти быстрее, чем сегмент коммерческих.

Облаца в регионах

Наряду с вариантами «строить самим» и «арендовать в коммерческом ЦОДе» есть и третий вариант получения необходимой ИТ-инфраструктуры – использование облачных сервисов. Сейчас на региональном облачном рынке можно проследить несколько тенденций. Во-первых, как отмечает Виктор Красноусов, директор центра региональных продаж B2B ГК «РТК-ЦОД», это усиление конкуренции облачных провайдеров, обусловленное ростом спроса со стороны как федеральных игроков, так и регионального бизнеса. Причем заказчики зачастую не просто покупают облачные услуги, но и используют провайдера как центр компетенций. В условиях высокой конкуренции неизбежны случаи ценового демпинга. Кроме того, провайдеры стараются формировать комплексные предложения. «Кто-то предлагает облака в комплекте с каналами, кто-то – с льготными кредитами», – делится наблюдениями В. Красноусов.



Виктор Красноусов, ГК «РТК-ЦОД»

Но при этом заказчики не готовы уходить полностью в классические облака. Неудивительно, что все больше провайдеров запускают решения типа «оборудование как сервис» (Bare Metal, HaaS). «Это говорит о том, что облако в чистом виде не отвечает задачам бизнеса, высоконагруженные системы требуют выделенных кластеров, – продолжает В. Красноусов. – Спрос на искусственный интеллект, на решения с GPU имеет отраслевую специфику. У нас есть реализованные проекты для медицины, для финтеха. Но покупать GPU компании не готовы, поэтому растет спрос на GPUaaS».

Третья тенденция – рост спроса на георезервирование. Если раньше такие решения рассматривали в основном заказчики из Москвы и Санкт-Петербурга, то сейчас и региональные компании все чаще интересуются разнесением ИТ-систем на большие расстояния. «Клиенты из Екатеринбурга запрашивают инфраструктуру в Новосибирске, клиенты из Санкт-Петербурга размещаются в ЦОДах Нижнего Новгорода», – говорит В. Красноусов.

Отдельно эксперт «РТК-ЦОД» указывает, что на фоне беспрецедентного роста числа кибератак повышается востребованность решений для гарантированного восстановления. В частности, выросло число запросов на ленточные библиотеки. На их основе

организуют отчуждаемые бэкапы, которые хранятся отдельно от «боевой» инфраструктуры и не связаны с ней по сети.

Проблемы роста

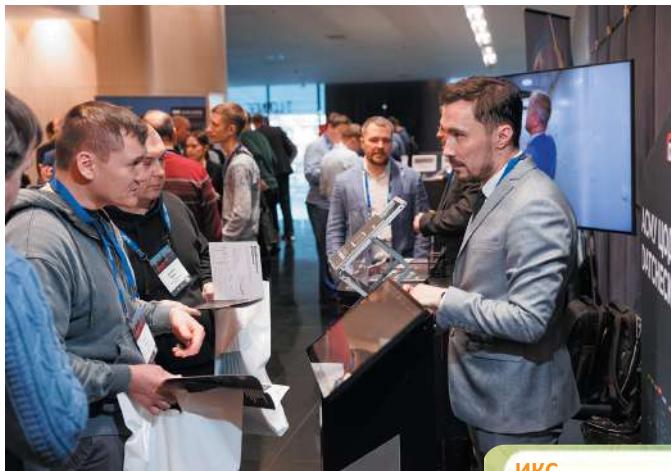
В мировом масштабе важной тенденцией, которую выделяет исполнительный директор компании «Ди Си квадрат» Александр Мартынюк, стало превращение гиперскейлеров в основных застройщиков ЦОДов. На Западе они строят огромные data-центры – мощностью в сотни мегаватт и даже несколько гигаватт на одной площадке.



Александр Мартынюк, «Ди Си квадрат»

Согласно данным Synergy Research Group, если в 2017 г. в ЦОДах гиперскейлеров размещалось около 10% критичной ИТ-нагрузки, то в 2023 г. этот показатель увеличился до 20%, а к 2029 г. вырастет до 40%. Если учитывать мощности, гиперскейлерами арендуемые, то он превысит 60%. Примечательно, что за рассматриваемый период доля корпоративных ЦОДов снизится с 60 до 20%.

А в России, где основные мировые гиперскейлеры отсутствуют, к строительству ЦОДов все активнее подключаются крупные девелоперы. Эту тенденцию отмечает Евгений Вирцер, основатель ГК Key Point: «Они поняли, что ЦОД – это дорогая технологическая недвижимость. Построить один ЦОД – все равно что 20 жилых комплексов, но денег проект ЦОДа приносит больше».



В выставочной зоне

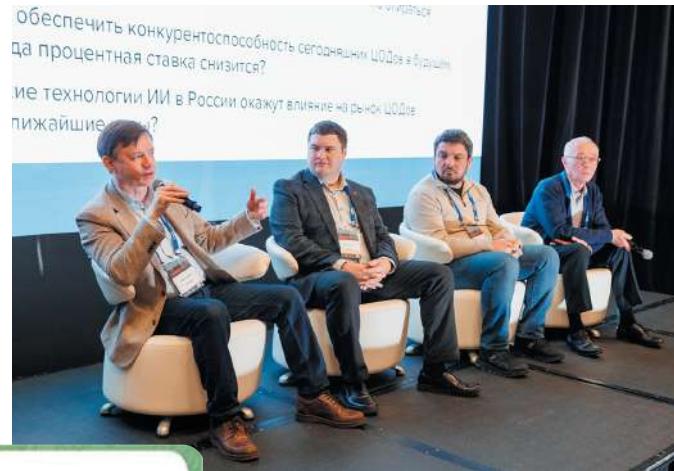
По данным Е. Вирцера, более половины введенных за последнее время стоек – это девелоперские проекты.

Основная болевая точка отрасли ЦОДов – энергетическая. В целом в мире энергопотребление ЦОДов растет значительно быстрее, чем возможности систем генерации энергии. Поэтому, обращает внимание А. Мартынюк, цодостроители все чаще прибегают к размещению своих площадок рядом с центрами генерации. «Да, при этом встают вопросы транспортной доступности и сетевой связности, но проекты создания ЦОДов рядом с АЭС возникают все чаще», – указывает он.

Во многом из-за проблем с энергетикой в ряде крупных мировых локаций ЦОДов, таких как Амстердам или Сингапур, строительство ЦОДов запрещено или серьезно ограничено. Это обостряет дефицит свободной емкости ЦОДов. Согласно данным, приведенным экспертом «Ди Си квадрат», в основных мировых локациях доля свободных мощностей варьируется от 1 до 5% – это очень-очень мало. Понятно, что дефицит стимулирует рост цен на услуги colocation, которые в среднем по миру увеличиваются за год на 15%.

Ставка на ЦОДы

Дефицит стойко-мест в коммерческих ЦОДах наблюдается и в России. Определяемый этим фактом рост стоимости соответствующих услуг усиливается из-за дорогих денег



На дискуссии «Отрасль ЦОДов: рынок, деньги и ИИ»

и другими экономическими проблемами, в любом секторе экономики в результате заплатит потребитель. В цодостроительстве велика доля здорового предпринимательского риска: заполнится ЦОД или нет? будут заказчики ждать потенциально дешевой стойки три-четыре года или будут брать то, что есть? по какой цене? Однозначных ответов нет. Единственное, что можно сказать точно, – инфраструктура будет вос требована», – рассуждает Е. Вирцер.

В проектах коммерческих ЦОДов на первом месте – окупаемость, возврат инвестиций. Сейчас, при нынешней ставке ЦБ, большинство экспертов оценивают среднее время окупаемости цодовских проектов в 10 лет. «Что будет через два года? Может быть, ставка упадет, стоимость услуг colocation повысится, и сроки окупаемости сократятся. А может, будет по-другому, и сроки окупаемости вырастут до 15 лет», – продолжает основатель Key Point.

При нынешнем уровне ключевой ставки экономика проектов «собирается» очень тяжело. И снижение общей стоимости владения за счет инженерной инфраструктуры, как подчеркивает А. Мартынюк, это возможность продвинуться на рынок. Поэтому инженерные компетенции команды так важны для успеха проекта в целом.

ИКС

Что способно в наибольшей степени стимулировать развитие отрасли ЦОД?

Анонимный опрос

- 53% Снижение ставки ЦБ (повышение доступности денег)
- 17% Ускорение темпов цифровизации экономики
- 6% Повышение доверия к услугам коммерческих ЦОД
- 9% Расширение ассортимента и повышение качества российских решений для ЦОД
- 8% Повышение доступности передовых зарубежных решений для ЦОД
- 4% Ничто не способно увеличить текущие темпы роста отрасли ЦОД
- 3% Другое

Результаты опроса в телеграм-канале «ИКС-МЕДИА»

(высокой ставки ЦБ). Именно это серьезно сдерживает реализацию новых проектов. Как показал опрос, проведенный в телеграм-канале «ИКС-Медиа», более половины респондентов считают, что снижение ставки ЦБ (повышение доступности денег) в наибольшей степени способно стимулировать развитие отрасли ЦОДов (см. рисунок). На втором месте – ускорение темпов цифровизации экономики. Пессимистов, считающих, что ничто не способно увеличить текущие темпы роста отрасли ЦОДов, оказалось всего 5%.

«За любую историю, связанную с повышением ставки, изменением курса

Александр Барков
Екатеринбург – Москва

ЦОДы в Узбекистане: как снять барьеры



Устранение проблем с энергоснабжением и введение ЦОДов в правовое поле способны значительно ускорить развитие цифровой инфраструктуры в Узбекистане и привлечь в страну новых игроков в области цдостроения.



Актуальные экономические и технические вопросы, связанные с ЦОДами, обсуждались на ставшем уже традиционным форуме Eurasia Data Center & Cloud Forum. Организованное «ИКС-Медиа» мероприятие, которое включало семинары, выставку и конференцию, посетили более 400 специалистов.

Одно из главных препятствий для строительства новых ЦОДов в Узбекистане, как констатировали многие эксперты, – трудность получения необходимых энергетических ресурсов. С 2018 г. в республике усугубляется дефицит собственных генерирующих мощностей. Проблемы электросетевого комплекса Узбекистана заключаются в высоком уровне износа распределительных сетей и подстанций и низкой автоматизации и цифровизации объектов электроэнергетики.

Однако эксперты отмечают большой энергетический потенциал Узбекистана, особенно в плане альтернативной энергетики. Более 300 солнечных дней в году и высокая интенсивность солнечного сияния открывают хорошие перспективы для развития солнечной энергетики, а ветровые условия в центральных и западных регионах – для ветроэнергетики. Бла-

гоприятна ситуация и для гидроэнергетики (имеется значительный ресурс для строительства малых и крупных ГЭС), и для атомной энергетики (по данным Всемирной ядерной ассоциации, Узбекистан – пятый по величине производитель урана в мире).

На возобновляемые источники энергии ориентируются и крупные инвесторы, приходящие на рынок ЦОДов Узбекистана. Так, компания DataVolt собирается построить в республике несколько ЦОДов, и все они будут работать за счет возобновляемых источников энергии. Первый data-центр мощностью 10 МВт будет создан на территории IT Park Uzbekistan в Ташкенте. Также в планах компании – строительство data-центра мощностью 250 МВт в Новом Ташкенте и объекта на 40 МВт в Бухарской области. Всего DataVolt планирует до 2030 г. направить на проекты в Узбекистане до \$5 млрд.

Спрос на услуги коммерческих ЦОДов в Узбекистане, как считает Фаррух Алимухамедов, заместитель генерального директора по развитию нового бизнеса компании East Telecom, опережает предложение. И главная причина, по его мнению, – уже упомянутая проблема получения электроэнергии. В качестве примера он привел один из запланированных крупных проектов своих коллег в Ташкентской области. «Государство

выделило землю. Был подписан протокол об энергообеспечении. На бумаге энергообеспечение должно быть, а по факту его нет, – рассказал он и резюмировал: – Как только эта проблема будет решена, начнется бум коммерческих ЦОДов». Еще один барьер для развития индустрии ЦОДов в Узбекистане – отсутствие в законодательстве республики определения ЦОДа как объекта критической инфраструктуры. Сама компания East Telecom уже в ноябре 2024 г. планирует запустить в эксплуатацию в Юнусабадском районе Ташкента первую очередь коммерческого ЦОДа, рассчитанного на 300 стоек.

«Если государство хочет развивать эту отрасль, оно должно сделать доступ к деньгам, к энергетике, к клиентам одинаковым для всех игроков», – считает Евгений Вирцер, основатель ГК Key Point. Эта компания развивает сеть региональных ЦОДов в России, а недавно объявила о строительстве data-центра в Казахстане. Присутствие Е. Вирцера на конференции в Ташкенте свидетельствует об интересе к этому рынку. Для инвесторов же важна следующая высказанная основателем Key Point мысль: «Если рассматривать ЦОД как недвижимость, то очевидно, что спрос на объект, в котором хранятся и обрабатываются данные, никогда не упадет».

**Александр Барсов
Ташкент – Москва**

НОВОСТИ ОТРАСЛИ

В Саудовской Аравии появится ЦОД мощностью 1,5 ГВт



DataVolt и проект Неом (Саудовская Аравия) подписали соглашение о разработке кампуса данных-центров мощностью 1,5 ГВт в промышленной зоне Оксагон, входящей в территорию Неома. Первоначальные инвестиции в проект составят \$5 млрд. Ввод кампуса в эксплуатацию будет осуществляться поэтапно. Ожидается, что первая очередь мощностью 300 МВт будет введена в эксплуатацию к 2028 г. Расположение Оксагона обеспечивает свободный доступ к подводным оптическим кабелям, что гарантирует быстрое и надежное интернет-соединение. В сочетании с доступной возобновляемой энергией и активно развивающейся промышленной экосистемой это делает город оптимальным для запуска крупномасштабного ИИ-ЦОДа.

В Норвегии вводятся правила «прозрачности» для ЦОДов

С 1 января в Норвегии начал действовать новый закон об электронных коммуникациях, согласно которому в стране создается реестр данных-центров. Операторы ЦОДов в срок до 1 июля должны представить информацию о себе в регулирующие органы. Новые данные-центры должны быть зарегистрированы до начала строительных работ. Компании, не соблюдающие законодательство, могут быть оштрафованы на сумму до 5% годового оборота. Норвегия утверждает, что является первой европейской страной, сдавшей национальный реестр данных-центров. Цель реестра – отделить «полезные» ЦОДы от криптомайнеров.

В Тверской области построят ЦОД мощностью 125 МВт

Компания Net One объявила о запуске проекта строительства ЦОДа в Тверской области. Наличие контракта на поставку трубопроводного природного газа позволит обеспечить электрогенерацию суммарной мощностью 125 МВт и реализовать не менее 10 тыс. серверных стоек ЦОДа уровней Tier III/Tier IV мощностью до 20 кВт на стойку. ЦОД на базе собственной электрогенерации будет построен на принадлежащей партнеру промышленной площадке в Тверской области. Проект предполагает поэтапный ввод. На пер-

НОВОСТИ АНО КС ЦОД



Встреча участников АНО КС ЦОД

23 января 2025 г. состоялась встреча учредителей, участников и ассоциированных партнеров АНО КС ЦОД. В неформальной обстановке собрались руководители крупнейших российских данных-центров и ключевые игроки отрасли. Присутствовали около 90 человек.

Заслушали доклад генерального директора Дмитрия Бедердинова о разработанных участниками АНО КС ЦОД отечественных моделях классификации и эксплуатации данных-центров и возможностях их использования при аттестации существующих и строящихся объектов, которая будет проводиться под эгидой и управлением общественной организации АНО КС ЦОД.

вом этапе планируется создать ЦОД на 2 тыс. серверных стоек.

MWS более чем вдвое увеличит мощности GreenBushDC

В декабре 2024 г. MTS Web Services (MWS) объявила о начале работ по расширению мегаЦОДа МТС в подмосковном Зеленограде – GreenBushDC. В ходе расширения в данных-центре появится более 650 новых стойко-мест, а его общая мощность вырастет более чем вдвое. Работы завершатся летом 2025 г. В новых стойках будет размещаться облачная инфраструктура MWS. В общей сложности у МТС 15 собственных данных-центров, пять из которых расположены в Московском регионе.

«РТК-ЦОД» планирует открыть данных-центр в Нижнем Новгороде

Соглашение о создании данных-центра было подписано генеральным директором кластера «РТК-ЦОД» Сергеем Бочкаревым и губернатором Нижегородской области Глебом Никитиным в 2023 г. на конференции ЦИПР. В 2024 г. стороны приняли решение о вводе в эксплуатацию 400 стойко-мест в первом полугодии 2025 г. В планах развития ЦОДа – расширение до 1 тыс. стоек, а также внедрение услуг облачного хранения для коммерческих организаций. Сегодня объекты «РТК-ЦОД» работают в Москве, Санкт-Петербурге, Новосибирске, Екатеринбурге, Удомле. Завершается строительство новых очередей данных-центров в Екатеринбурге и Нижнем Новгороде, начато строительство ЦОДа в Хабаровске.

Модульный ЦОД в Волгоградской области



Компания GreenMDC по заказу ГК Softline разработала и поставила масштабируемый модульный ЦОД для Комитета финансов Волгоградской области. При выборе оборудования заказчик учитывал будущий переезд организации в другое административное здание. Поэтому решение МЦОДа предусматривает перемещение на новое место в короткие сроки с минимальными трудозатратами. Производство, поставка и сборка МЦОДа заняли пять месяцев. Перед отправкой на площадку заказчика данных-центр был протестирован с имитацией 100%-ной нагрузки на заводе в Санкт-Петербурге.

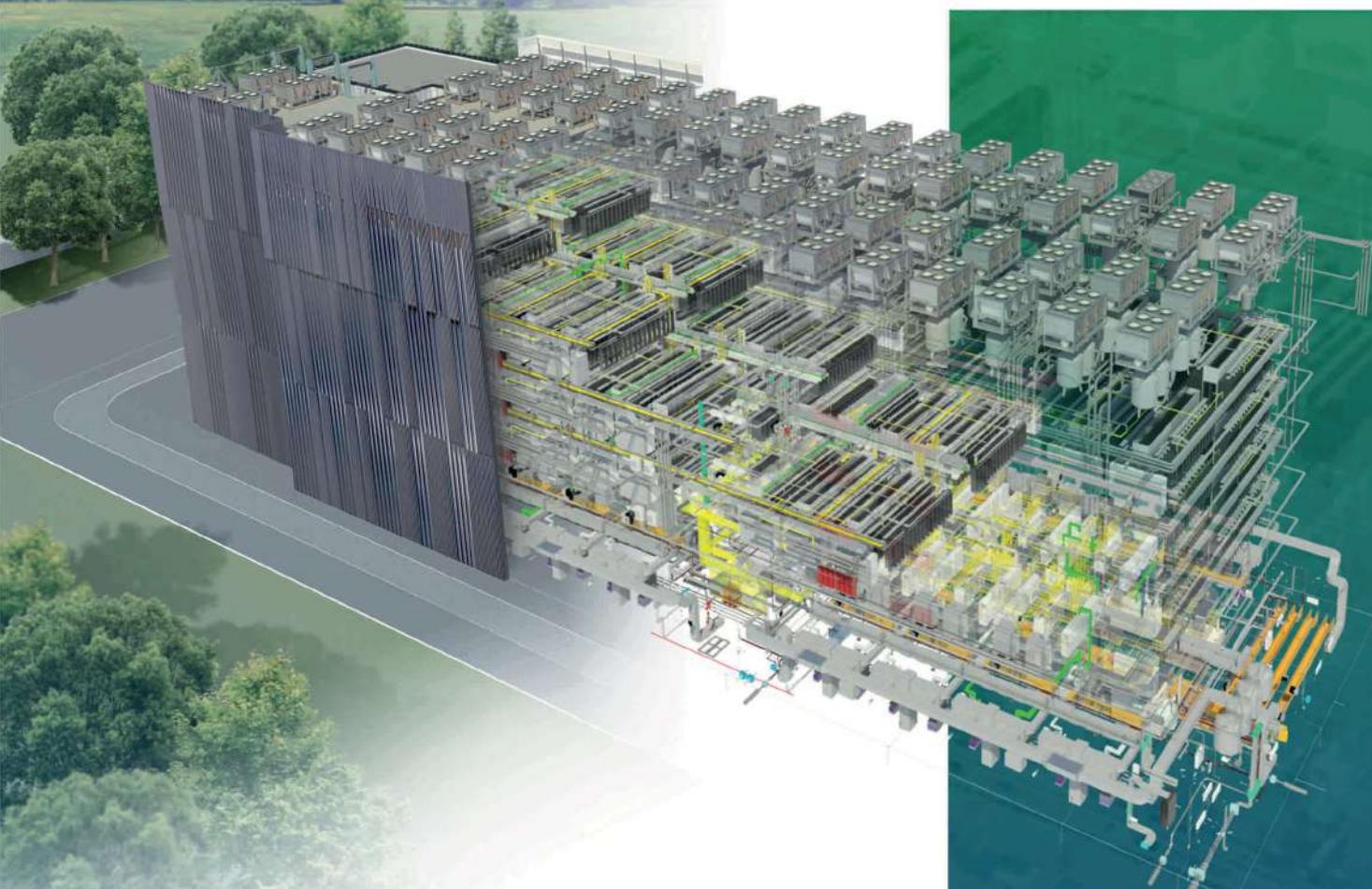
В Узбекистане построят ИИ-ЦОД

Индийская компания Larsen & Toubro (L&T) построит в Ташкенте данных-центр мощностью 10 МВт. По заявлению L&T, проект установит новые стандарты для инфраструктуры данных-центров в регионе. В нем будут использованы передовые технологии, в том числе в области безопасности и защиты персональных данных, а также соблюдаются требования устойчивого развития. Речь идет о минимальном воздействии на окружающую среду и высокой энергоэффективности.



СВОБОДНЫЕ
ТЕХНОЛОГИИ
ИНЖИНИРИНГ

ПРОСТЫЕ РЕШЕНИЯ СЛОЖНЫХ ЗАДАЧ



ПРОЕКТИРОВАНИЕ
И СТРОИТЕЛЬСТВО
ДАТА-ЦЕНТРОВ



ЦОДы в условиях дефицита электроэнергии



Спрос на услуги дата-центров стремительно растет, и не менее стремительно растет их энергопотребление. Производство же электроэнергии увеличивается значительно медленнее, и грядущий дефицит заставляет ЦОДы разрабатывать альтернативные сценарии развития.



**Сергей
Вышемирский,**
технический
директор,
IXcellerate

Основная причина роста востребованности ЦОДов – big data. Сегодня, по оценке Statista, ежедневно генерируется 328,77 млн Тбайт данных, а глобальные прогнозы на 2025 г. достигают 180 Збайт. И все эти данные нужно где-то обрабатывать и хранить. Не менее важный катализатор спроса – искусственный интеллект. Для реализации его потенциала к концу текущего десятилетия только в США понадобится дополнительно создать инфраструктуру ЦОДов мощностью 50–60 ГВт. К этому моменту потребности центров обработки данных в электроэнергии, согласно McKinsey Research, вырастут примерно в три раза по сравнению с текущими. Многие эксперты опасаются, что рост энергопотребления, связанный с распространением больших языковых моделей, вскоре превысит возможности энергетических компаний. В отчете Gartner говорится, что спрос на электроэнергию в сфере ИКТ до 2030 г. будет увеличиваться на 25% ежегодно, в то время как глобальное производство электроэнергии – всего на 3%.

Очевидный дисбаланс – серьезный повод для беспокойства. Неизбежным результатом грядущего дефицита станет повышение цен на электроэнергию, увеличение эксплуатационных расходов и себестоимости услуг data-центров. Самый пессимистичный прогноз – замедление темпов роста всей индустрии. В условиях повышающегося спроса на электроэнергию и ограниченной доступности энергомощностей центры обработки данных разрабатывают альтернативные сценарии роста.

Смена геолокации

Провайдеры услуг ЦОДов все чаще задумываются о переносе своих объектов в регионы с недорогим электричеством, например, рядом с ГЭС или АЭС. Близость к источникам генерации позволяет оптимизировать расходы на сетевую составляющую и отказаться от дорогостоящих и нездоровых методов резервирования, таких как ДГУ. Еще одной альтернативой могут стать регионы со стабильным климатом: суровые погодные условия значительно снижают энергопотребление систем охлаждения.

Альтернативные источники энергии

Дата-центры уже не один десяток лет используют «зеленые» технологии, в том числе возобновляемые источники энергии. Это и ветровые электростанции, и солнечные фермы, и геотермальные электростанции. Примеров подобных инициатив становится все больше, однако единственным надежным источником, способным бесперебойно обеспечивать энергию, являются АЭС. Будущее индустрии ЦОДов во многом связано с использованием атомной энергии, в том числе с созданием собственных микрореакторов.

Использование избыточного тепла

Расположенные в машинных залах серверы выделяют тепло, которое провайдеры услуг ЦОДов могут использовать для собственных нужд, например, направлять тепловую энергию систем кондиционирования на обогрев своих объектов. Несколько крупных data-центров в Европе пошли еще дальше: они передают теплоизбытки коммунальным службам и функционируют как элемент городской отопительной инфраструктуры. Использование «ненужного» тепла становится фактором экономии бюджета и для самих data-центров, и для муниципальных властей.

Инновационные системы охлаждения

Поддержание необходимых температурно-влажностных условий в машинном зале сопряжено с большими затратами: на охлаждение серверной инфраструктуры уходит около 40% всей энергии, потребляемой data-центром. Повысить энергоэффективность можно применением инновационных решений. В их числе – жидкостное охлаждение (позволяет снизить энергопотребление за счет отказа от вентиляторов и максимально увеличить производительность GPU и CPU) и системы естественного охлаждения (фрикулинг), которые используют наружный воздух для охлаждения серверных.

Энергоэффективные технологии

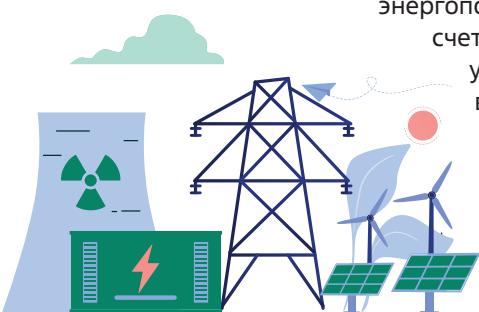
В числе других энергоэффективных технологий – источники бесперебойного питания с повышенным КПД (выделяют меньше тепла, а значит, меньше электроэнергии требуется на их охлаждение), литий-ионные аккумуляторы (обладают меньшим тепловыделением, а значит, снижается потребность в охлаждении воздуха), аккумуляторы на базе гибридных суперконденсаторов (HSC), которые обладают высокой мощностью и не нуждаются в дополнительном охлаждении, а также батареи длительного хранения энергии (LDSB), которые способны обеспечивать мощность от нескольких киловатт до мегаватт.

Системы хранения энергии (ESS)

Технологии ESS позволяют ЦОДу эффективно управлять расходами на электроэнергию. Они дают возможность аккумулировать электроэнергию в периоды низких тарифов и использовать ее в моменты пикового потребления. Кроме того, ESS выступают в роли резервного источника питания, что значительно увеличивает надежность и устойчивость работы data-центра в случае перебоев с электроснабжением от сети.

Рынок коммерческих ЦОДов – достаточно гибкая конструкция, которая быстро меняется в зависимости от запросов клиентов, и его игрокам сложно отказать в прозорливости и стратегическом видении. Внедрение новых технологий и оптимизация ресурсов не останавливаются ни на минуту, чтобы соответствовать требованиям времени. Однако ограничить

энергопотребление и повысить эффективность ЦОДа невозможно исключительно за счет усилий его оператора. Для этого необходимы согласованные действия всех участников процесса создания, хранения и потребления данных. Не менее важно внедрение стандартов энергоэффективности. В Европе, например, многие компании дополняют условия тендеров обязательным наличием «зеленого» сертификата, подтверждающего, что не менее 50% основного энергоснабжения ЦОДа идет из возобновляемых источников энергии. Аналогичные требования предъявляют инвесторы. Список можно продолжить, но и приведенных примеров достаточно, чтобы понять: без создания энергоэффективной экосистемы потенциал инновационных технологий не будет реализован в полной мере. **ИКС**





модели
сервисы
инфраструктура

2-й ежегодный форум

Новосибирск 16 апреля 2025

Grand Autograph Hotel Novosibirsk

Новосибирск – один из основных центров цдостроения в России. Конференция посвящена обсуждению актуальных вопросов развития индустрии ЦОДов как в самом Новосибирске, так и в целом в Сибирском и Дальневосточном федеральных округах. Традиционно рассматриваются российские и мировые тенденции, практические вопросы проектирования, построения и эксплуатации ЦОДов, а также предоставления на их базе услуг, в том числе облачных.

В фокусе форума:

- Рынок ЦОДов и облаков. Аналитика от iKS Consulting
- Экономика и бизнес-модели, новые проекты
- Модульные, контейнерные и prefab-ЦОДы
- Инженерная инфраструктура дата-центров
- Системы генерации и накопления электроэнергии

РЕКЛАМА / 16+



подробно о программе и
участниках на сайте форума
nsk.dforum.ru



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

ЦОДы – дело жизни

ЦОДы как дети. Важно помочь им вырасти, пройти все этапы от концепции до сдачи в эксплуатацию. Непростая задача, особенно в нынешних условиях. Как ее решает команда «Ди Си квадрат», рассказывает основатель и исполнительный директор компании Александр Мартынюк.



– Александр, с чего все начиналось? Когда вы построили первый ЦОД? Как возникла «Ди Си квадрат»?

– Мой первый ЦОД – это вычислительный центр для госзаказчика, проект, в котором я участвовал в 1996–1998 гг. Он обладал всеми атрибутами ЦОДа – критическая информация, резервирование систем электропитания, охлаждения, каналов связи, высокая степень автоматизации, но понятия «ЦОД» еще не было.

Первые настоящие ЦОДы я увидел в начале нулевых в Англии и США. Это были объекты HSBC, ABN AMRO, DataGuard, Credit Swiss... И это был космос по сравнению с тем, что делали мы: другой уровень сложности, качества, автоматизации. Это были действительно объекты критической инфраструктуры, где стояли бизнес-критичные системы. И вот тогда я влюбился в ЦОДы, понял, что хочу заниматься именно ЦОДами, хочу создать компанию, с которой можно это делать.

Команда будущей компании «Ди Си квадрат» начала формироваться в 2000 г. Мы вместе реализовали несколько проектов, в том числе для корпоративного ЦОДа ТНК-BP* в 2004 г., а в 2008-м выделились в отдельную компанию. Первым крупным проектом стало участие в создании штаб-квартиры ВТБ в башне «Федерация» в Москва-Сити. Начали с нескольких инженерных систем для ЦОДов (их там было три, в том числе один для трейдеров), но потом заказчик поручил нам работу над всей инженерной инфраструктурой. Башня «Федерация» – действительно сложный проект, который помог нам достаточно быстро приобрести репутацию компании, умеющей управлять сложными проектами.

– **Что означает слово «квадрат» в названии?**

– Сказался математический склад моего ума. Первое dc – это data centers, второе – design and consulting. Получается dc в квадрате, чистая математика, ничего сакрального.

– **Если оперировать общепринятыми терминами, то «Ди Си квадрат» – это консультант, эксперт, проектировщик, интегратор, управляющая компания?..**

– По мере развития компании мы расширяли свой функционал. На данный момент делаем все, кроме проектирования, монтажа и эксплуатации ЦОДов. Мы ЦОДы придумываем, подыскиваем для них площадки, формируем технические решения, подбираем вендоров, организуем конкурсные процедуры, управляем проектами, сопровождаем их реализацию, участвуем в сертификации, принимаем участие в создании службы эксплуатации, разрабатываем финансовые модели, помогаем защищать их в банках.

Мы выполняем функции управляющей компании, технического консультанта, проектного офиса заказчика и т.д. Но позиционируем себя в первую очередь как экспертную компанию. Потому что имеем экспертные знания в этой узкой и глубокой области во всем спектре

* См.: А. Мартынюк «Нам нужно, чтобы у заказчика было лучшее решение». «ИКС» № 1'2023, с. 16.

задач. Мы понимаем ЦОДы со всех сторон и на всех стадиях – от идеи до эксплуатации и продажи.

– Почему вы не берете на себя проектирование? Это же не самое сложное.

– Нам интересна творческая, интеллектуальная сторона от самого начала: идеи, концепции будущего ЦОДа. Проектирование же больше процессная вещь, доступная услуга: на рынке немало компаний, занимающихся проектированием. Можно нанять несколько команд проектировщиков и координировать их работу, чтобы оптимизировать процесс проектирования. При этом, конечно, мы будем контролировать, чтобы проектная документация была разработана в соответствии с первоначальной идеей, успешно прошла сертификацию Uptime Institute, была потом реализована «в бетоне и металле» и объект получился таким, каким мы с заказчиком его придумали.

– Технологии или экономика проекта: что ставите на первое место?

– Мы предлагаем технические решения, исходя из их экономической целесообразности. Мы приземленные люди, стремимся к максимально сбалансированному в плане техники и денег проекту и не предлагаем того, что заведомо будет очень дорого.

Например, излишне высокий уровень резервирования стараемся не предлагать, избыточность в оборудовании ведет к увеличению CAPEX и к длительной окупаемости. С другой стороны, важно понимать, что большее количество меньших по мощности источников при распределенном резервировании, например $(7/6)N$ против $(4/3)N$, может усложнить эксплуатацию. Если заказчик к этому готов, то просчитываем такие схемы. Здесь нужен баланс.

Многое надо учитывать. Так, применение неизвестного, более дешевого оборудования вынуждает для обеспечения необходимой надежности закладывать больший ЗИП, что повышает затраты. А поставка по «серым» каналам приводит к тому, что вы не



Екатерина Нигай,
руководитель проектов

Про компанию

Это огромная часть моей жизни, путь длиной более чем в 20 лет. Для меня «Ди Си квадрат» – это высокий профессионализм, человеческие отношения и уникальный стиль руководства, где внутренняя ответственность, взаимоуважение и доверие важнее регламентов и «распоряжений».

Про трудности

Есть определенная недооценка роли независимых отраслевых экспертов в планировании и реализации проекта. Не всегда это недооценка со стороны заказчиков: они-то, если обращаются к нам, видят реальную пользу и экономию. Но важно внутри проекта наладить коммуникации с другими участниками: генпроектировщиком, генподрядчиком, системным интегратором...

Технологии или экономика

Мы часто «пляшем» от экономики. Важно подсказать заказчику, чего можно достичь в рамках бюджета, а чего нет. И не браться за невозможное, не обнадеживать только ради того, чтобы остаться в проекте. Но технологии, корректно подобранные «физика», начиная с земельного участка и заканчивая эксплуатационными особенностями конкретного решения, непосредственно влияют на экономические показатели проекта.

получаете гарантии и сервисного партнера. Значит, рискуете.

ЦОД – это деньги. Коммерческий ЦОД должен окупаться. А в корпоративных проектах внутреннюю экономику надо защищать, потому что заказчик сравнивает, что ему выгоднее: строить самому или арендовать ресурсы в коммерческом ЦОДе. Техника и деньги всегда идут рука об руку. Мы это прекрасно понимаем. В отличие от тех, кто просто рисует эскизные проекты.

– Представьте, пожалуйста, свою команду. Как сегодня решаете кадровые проблемы (если они, конечно, возникают)?

– Очень уважаю своих ребят, дорожу ими – и теми, с кем работаем много лет, и теми, с кем совсем недавно. В нашей команде люди определенного склада характера. Самоорганизованные, потому что мы работаем без офиса и у нас ненормированный рабочий день. Уравновешенные и неконфликтные. Наши подрядчики, уровень их подготовки, уровень подготовки заказчиков очень разные, поэтому острые вопросы возникают часто, и если включать эмоции или инженерное это, то ничем хорошим это не закончится. Важно уметь спокойно, профессионально и аргументированно обосновывать свою точку зрения, не повышая голоса и не переходя на личности.

Важно и то, что многие, кто у нас работает, занимались эксплуатацией ЦОДов, понимают, какое оборудование с какой стороны обслуживается, что удобно, что неудобно, что надо предусмотреть в плане монтажа, подходов, складов ЗИП. Проектировщик может прекрасно готовить проектную документацию, но он никогда ничего не обслуживал, не монтировал, у него нет опыта, и взгляд у него другой – как на буклет. В свою очередь, монтажники ничего не эксплуатируют, они исходят из того, что им нужно смонтировать и сдать. Как с этим дальше будет жить заказчик, их не интересует.

Мы идем «от заказчика» с учетом опыта проектирования, сертификации и эксплуатации. И такого симбиоза,

взаимодополняющей экспертизы на рынке практически ни у кого больше нет. В итоге отличия проектов, которые сдаем мы, от всех других видны невооруженным глазом. И сертификаты Uptime это подтверждают. Только в прошлом году успешно прошли три сертификации объектов (Facility), а работы по сертификации проектов (Design) фактически не прекращаются никогда.

– Есть ли у вас предпочтения в выборе проектов, заказчиков?

– К нам приходят с проектами трех основных типов. Первый – когда у заказчика и/или инвестора есть деньги и он хочет построить ЦОД. Или не ЦОД. Так было с «Д9» (первым в России ЦОДом Tier IV. – Прим. ред.), изначально на площадке хотели построить склад или зарядную станцию для электромобилей. Но мы просчитали экономику и показали заказчику, что кейс с ЦОДом гораздо интереснее. Хорошо, когда есть идея и у инвестора есть понимание, желание и возможность запустить проект. Мы с удовольствием включаемся с этапа -1: помогаем разрабатывать концепцию, подбирать площадку, формировать команду, видение, эскизный проект и т.д. Это лучшее из того, что может быть. В этом случае мы можем сделать для заказчика максимум. Да, могут быть ограничения площадки или внутренние ограничения заказчика, но у нас не связаны руки в выборе технических решений, компоновки, мы можем предложить оптимальный вариант, снизить CAPEX, обеспечить максимальные эксплуатационные надежность и удобство. Короче, сделать отличный проект.

Это не означает, что, когда надо вписаться в существующее здание (brownfield), получится плохой проект. Там больше ограничений, и это несколько другая работа. Кстати, до 2020 г. большинство проектов были именно brownfield. Проекты «в чистом поле» (greenfield) начались сравнительно недавно.

Второй тип проекта – когда заказчик начал проектирование, но дальше проект «не идет». Экономика не со-



Максим Важенин,

ведущий эксперт
по системам
электроснабжения

Про компанию

В этом году исполнится 20 лет, как познакомился с Александром и Екатериной. Знакомство состоялось на строительстве data-центра для оператора мобильной связи. Александр с командой консультировал, сопровождал проектирование и контролировал реализацию проекта, а я был на стороне заказчика. С той поры и по сей день вместе работаем над разными проектами для разных сегментов и заказчиков. Весь путь «Ди Си квадрат» у меня перед глазами, потому отношение к компании очень личное.

Про основные тенденции

Во-первых, проекты укрупняются: сейчас реализуются ЦОДы на несколько тысяч стойко-мест и повышается мощность стойко-места – 10 кВт и более. Во-вторых, растет активность девелоперов и госкорпораций в освоении рынка ЦОДов. В-третьих, идет передел рынка оборудования инженерных систем после ухода западных мейджоров.

Про трудности

Трудности бывают всегда, но всегда нужно находить окна возможностей, варианты решений и способы ухода от проблем... Из чувствительного в данный момент – определенные сложности с ассортиментом, функционалом, качеством, документированностью, техподдержкой доступного на рынке инженерного оборудования.

дится, технические решения друг с другом не стыкуются, подрядчики не общаются, заказчик не понимает, что происходит, платит деньги, а результата нет. Мы выполняем работу «скорой помощи», включаемся в проект, анализируем текущий статус и начинаем выстраивать процессы: корректируем технические решения, организуем рабочее взаимодействие между подрядчиками, формируем рабочую схему с календарным графиком, словом, возвращаем проект в рабочее состояние. Дальше доводим проект до конца, помогая заказчику в пределах согласованных объемов и в рамках наших многочисленных компетенций, начиная с контроля проектирования и заканчивая операционной моделью эксплуатации объекта.

Третий тип проектов – техническая экспертная оценка, due diligence. Например, перед приемкой ЦОДа заказчик просит нас проверить, как выполнены работы, насколько они соответствуют проектной документации, есть ли нарушения, ошибки. Мы проводим «дью дил», готовим отчет с фотоматериалами, и заказчик на его основании разговаривает с подрядчиком о приемке работ, формирует ведомость доделки и т.д. Ту же самую процедуру часто выполняем в рамках сделок M&A. Проверяем сам ЦОД, его службу эксплуатации, регламенты обслуживания и готовим заключение, которое ложится в основу решения о том, будет объект покупаться или нет, какие у него недостатки, сколько стоит их устранение и т.д.

Есть и другие проекты. Например, анализ проектных решений для 100-мегаваттной майнинговой фермы. Такие вещи тоже делаем. Это точечный консалтинг.

– Насколько велика конкуренция на российском рынке цдостроения? Или профессиональных команд настолько мало, что конкуренция вообще не ощущается?

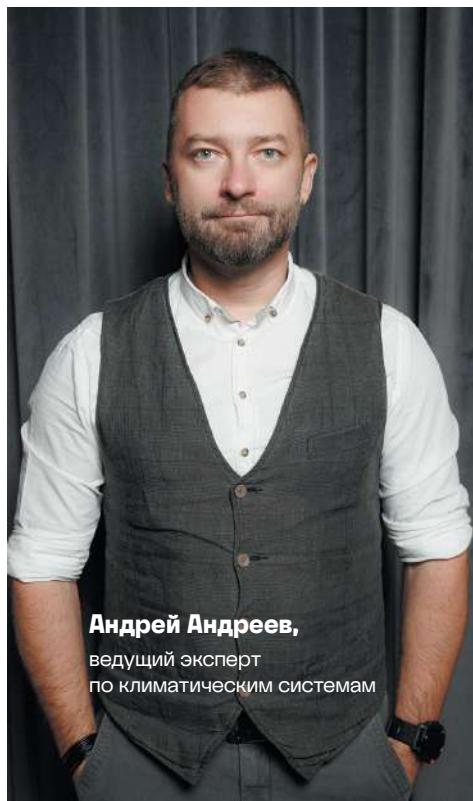
– Конкуренция существует, но не лобовая. Есть компании, которые берутся за подобную работу, но для них это не основной бизнес. Например, дистрибуторским компаниям

главное – заполучить клиента, чтобы потом продать ему оборудование. Отсюда – низкая стоимость их услуг, да и низкое качество. У них просто нет специалистов нужного уровня. Они не могут проработать и сформировать оптимальные технические решения. Как правило, у них есть определенный набор проектных решений, которые они пытаются «пристроить» к тому проекту, который удалось получить.

Взять, например, эскизный проект – важнейший документ, на основе которого заказчик принимает решение об инвестициях. Часто заказчик приходит к нам с проектом, в котором есть планировки, визуализации, черновик генплана, краткая пояснительная записка с указанием моделей оборудования – и, как правило, все. Эскизный проект, который делаем мы, кроме перечисленного содержит схемы для основных инженерных систем, матрицы оборудования, основные технические расчеты и т.д. При этом мы ориентируемся на решения, которые можно реализовать на оборудовании двух-трех производителей со схожими характеристиками. Такой документ формирует техническое решение. Зачастую реализуемый ЦОД фактически не отличается от нашего первоначального концепта. Для ЦОДов, построенных на основе наших эскизных проектов, попадание в бюджет – $\pm 5\%$. Это очень высокая точность, ведь в эскизном проекте нет расчета кубатуры бетона, тонн арматуры, конкретной спецификации оборудования. На основе своего опыта мы можем достаточно точно сформировать бюджет и календарный график реализации проекта, который тоже должен прилагаться к эскизному проекту. Кроме того, в контур эскизного проекта мы включаем графики финансирования и загрузки.

– Получается, что формирование эскизного проекта – важнейшая стадия проекта?

– Каждый этап важен. На каждом этапе своя цель. И если ты ее достиг, то в итоге получится гораздо лучше, чем ожидаешь. А если на первых этапах сэкономил и считаешь, что главное – купить оборудование, то ничего хо-



Андрей Андреев,
ведущий эксперт
по климатическим системам

Про компанию

Команда профессионалов высокого уровня позволяет не только индивидуально самореализоваться, но получать новые знания и опыт. Создана очень комфортная атмосфера, в основе которой полное доверие. Голос каждого сотрудника важен. Это помогает совместно вырабатывать действительно оптимальные решения.

Про особенность работы

Мы позиционируем себя как вендорнейтральную компанию, которая проводит независимую экспертизу проекта, технических решений. Выступаем техническим арбитром между заказчиком и проектировщиком, между заказчиком и строителем. Подобный технический надзор за проектами – уникальная специализация для нашего рынка.

Технологии или экономика

Мне важны изящество технических решений, их эффективность, ремонтопригодность. Но в рамках бюджета проекта. Бывает, что желаемые заказчиком технические решения не укладываются в бюджет, который он готов выделить. Тогда нужно искать компромисс.

рошего не получится. Покупка оборудования – это вообще самое простое. Конечно, важно купить хорошие продукты, чтобы готовить вкусный обед. Но если ты не умеешь готовить, то вкусный обед не сделаешь, какие бы прекрасные продукты ни купил.

– Какие изменения, происходящие на российском рынке ЦОДостроения, вы можете выделить?

– ЦОДы стали более гибкими с точки зрения применяемых технических решений и размещаемого оборудования. Для нас это вызов, мы должны придумывать более адаптивные и гибкие решения, чтобы иметь возможность размещать высокоплотные стойки с разными технологиями охлаждения. Но опыт показал, что мы способны такие задачи решать. Уже реализованы проекты, в которых можно комбинировать в машзале стойки на 5, 10, 15 кВт, ставить межрядные кондиционеры, делать системы прямого жидкостного охлаждения с подачей жидкости на охлаждающие пластины, установленные в серверах. И это все в рамках одного ЦОДа. Накапливаем наработки на будущее, понимая, куда движется техника и каковы запросы инвесторов. Но гибкость – это основное.

– Что для вас значит «Ди Си квадрат»?

– Для меня – дело жизни. Я душу вкладываю и в команду, и в проекты, и в нашу отрасль. Я действительно все это очень люблю. Это тот самый икигай (японская философия, помогающая находить удовлетворение, радость и осознанность во всех делах каждый день. – Прим. ред.), когда знания, опыт, возможности и оплата – все сходится в одной точке.

Для меня любой ЦОД как ребенок. Ему не должно быть плохо, его нужно заботливо вырастить и вложить в него все, что мы с командой знаем. Мы доводим его до «совершеннолетия», до запуска в эксплуатацию.



dcxdc.ru

Цифровые ассистенты и прогнозные модели: ИТ-тренды в промышленности 2025 года

Отечественный рынок ИТ насчитывает десятки тысяч программных и аппаратных решений для разных отраслей. При таком богатстве выбора правомерен вопрос: на что ориентироваться, на какие технологии обратить внимание, чтобы вывести цифровизацию компании на новый уровень?

Количество наименований в реестре российского ПО, как сообщил в сентябре 2024 г. на Kazan Digital Week премьер-министр России Михаил Мишустин, превысило 22 тыс. По оценке консалтинговой компании «Яков и партнеры», в 2023 г. объем ИТ-рынка в России увеличился на 10–15% – при среднемировых темпах роста в 7–8% – и достиг 3 трлн руб. А за первые полгода 2024 г. он, согласно исследованию НИУ ВШЭ, прибавил 63,2% в годовом исчислении и достиг 1,7 трлн руб.

Решения на базе искусственного интеллекта

Системы на основе ИИ уже сейчас применяются в промышленности для оптимизации использования ресурсов, технологических и бизнес-процессов. С их помощью автоматизируют рутинные задачи и снижают нагрузку

на персонал. Какие же решения наиболее перспективны в 2025 г.?

Цифровые ассистент-системы – одно из наиболее сложных программных ИИ-решений. Их используют, чтобы частично или полностью автоматизировать технологические и бизнес-процессы. Существуют разные ассистент-системы: от голосовых помощников до чат-ботов. В бизнесе последние два года набирают популярность цифровые помощники на базе больших языковых моделей (LLM).

Благодаря тому, что LLM понимают тексты на естественном языке и могут их генерировать, они позволяют:

- систематизировать данные и осуществлять быстрый поиск необходимой информации;

Максим Милков,
руководитель ИИ-направления,
Softline Digital (ГК Softline)

Антон Салин,
директор по продажам,
Softline Digital (ГК Softline)

- генерировать код, тестовые сценарии и синтетические данные для обучения других ИИ-моделей;
- составлять в реальном времени ответы на обращения в службу клиентской поддержки;
- оценивать эффективность текстовой и голосовой коммуникации сотрудников с клиентами;
- разрабатывать тренинги и контрольно-оценочные материалы для сотрудников.

Языковые модели способны на десятки процентов снизить затраты на рутинные операции. Что касается оптимизации техпроцессов в промышленности, то даже рост эффективности на 0,5–1% на одном из производственных участков приносит десятки миллионов долларов в год за счет увеличения объема производимой продукции. Поэтому цифровые ассистент-системы – это эффективный инструмент оптимизации ресурсов.

Системы прогнозирования и анализа данных занимают прочное место среди основных факторов успеха предприятий в разных отраслях. При грамотном подходе они обеспечивают высокую точность прогнозирования параметров производства и бизнес-процессов, позволяют снизить издержки, улучшить качество продукции и управление ресурсами.

По оценке McKinsey, предиктивные системы технического обслуживания увеличивают срок работы промышленного оборудования на 20–40% и сокращают время простоев на 30–50%. Кроме того, прогнозирование и анализ данных помогают в принятии решений, мониторинге рынка и стратегическом планировании.

Сейчас особенно востребованы модели прогнозирования различных рыночных показателей: динамики цен, спроса и предложения. Такие модели, созданные на базе машинного обучения, могут строить для бизнеса точные прогнозы на перспективу полугода-двух лет. Есть запрос и на разработку систем оптимизации производственных процессов, позволяющих повысить эффективность оборудования и маржинальность выпускаемой продукции.

среднем на 37,87% ежегодно, достигнет \$130,77 млрд.

Цифровые двойники набирают популярность благодаря тому, что это универсальный инструмент для оптимизации различных процессов. Однако перед их внедрением бизнес должен четко понимать свои цели: для чего компании нужен цифровой двойник и насколько его разработка целесообразна. Только в этом случае не возникнет трудностей с выбором задач и оценкой экономического эффекта данного инструмента.

Управление рисками при использовании ИИ

Специалисты сходятся во мнении, что искусственный интеллект нельзя использовать безоглядно из-за рисков, связанных с непрозрачностью таких систем и отсутствием ясности

программные решения, актуальные данные и помогают контролировать все стадии производства, а также оперативно принимать управленческие решения.

Готовые решения промышленной автоматизации позволяют компаниям ускорить внедрение технологий, снизить затраты на разработку и обслуживание систем и обеспечить адаптацию к современным требованиям. Но есть и ограничения: например, готовые решения по умолчанию подразумевают ограниченную кастомизацию и масштабируемость. Они не всегда способны удовлетворить индивидуальные потребности производств, поэтому требуют адаптации.



Отечественная ИТ-индустрия продолжает эволюционировать, пред-



Цифровые двойники – виртуальная модель реального объекта, процесса или системы. На основе данных цифровые двойники воспроизводят состояние и изменения тех явлений, чьими копиями являются. Главная задача этой технологии – мониторинг и оптимизация работы объекта, например, целого завода или отдельного цеха. Вместе с тем цифровые двойники умеют прогнозировать возможные сценарии производства и проверять гипотезы с помощью анализа «что, если».

Согласно данным ИСИЭЗ НИУ ВШЭ, в 2022 г. эту технологию использовали лишь 3,3% промышленных предприятий в России. Однако эксперты ожидают активного роста рынка цифровых двойников. Так, консалтинговая компания Mordor Intelligence в 2024 г. оценила объем рынка в \$26,25 млрд, а по прогнозам, к 2029 г. эта цифра, увеличиваясь в

правовом регулировании. Поэтому при создании и внедрении решений на основе ИИ особую важность приобретают доверие и управление безопасностью и рисками в этой сфере.

Например, все проприетарные, облачные ИИ-модели не являются безопасными, так как никто не мешает им собирать и хранить получаемые для работы чувствительные данные, хотя это может и противоречить локальным правовым актам. Безопаснее модели с открытым исходным кодом, которые запускаются локально или в закрытом контуре.

Автоматизированные системы управления

Тренд на использование отечественных автоматизированных систем управления технологическими процессами сохраняется. Системы промышленной автоматизации включают в себя оборудование,

лагая готовые и кастомизированные решения специфических потребностей предприятий. Основной задачей бизнеса становится поиск баланса между цифровизацией и ее практической целесообразностью. Сегодня ключевые тенденции в области промышленных технологий тесно связаны с применением искусственного интеллекта. Умные системы и гаджеты не ограничиваются автоматизацией повседневных задач и становятся важным элементом оптимизации рабочих процессов.

Успешное внедрение ИТ-решений требует четкого понимания бизнес-целей, грамотного управления рисками и выбора подходящих технологий. В условиях стремительного развития рынка ИТ взвешенный выбор подходящих решений станет основой для конкурентоспособности и устойчивого роста компаний. **ИКС**

ЦОД как сервис – услуга стала доступнее

«Цифровой остров» предлагает развертывание модульного data-центра на территории заказчика и его аренду по сервисной модели. На вопросы издания отвечает управляющий партнер компании Тимур Нугманов.



– Тимур, расскажите о компании «Цифровой остров». Когда она возникла и почему?

– «Цифровой остров» появилась в прошлом году как ответ на потребность рынка в быстром развертывании и дальнейшем сопровождении data-центров на площадке заказчика. Некоторые компании не могут пользоваться услугами коммерческих data-центров и облаков – в силу требований регуляторов, собственных политик безопасности или по экономическим соображениям. И при этом они не обладают экспертизой для строительства и эксплуатации ЦОДа. Таким компаниям мы предлагаем услугу «Дата-центр в аренду» (Data Center as a Service, DCaaS) – быстро доставляем и собираем ЦОД на территории заказчика, а затем занимаемся его мониторингом и обслуживанием.

– Почему компанию назвали «Цифровой остров»?

– Было много вариантов – хотелось название, связанное с цифровыми технологиями и обособленностью. Выбрали «Цифровой остров», что также ассоциируется с безопасностью, которой мы придаём большое значение. Слоган компании: «Безопасное пространство для ваших данных».

– Можно ли считать «Цифровой остров» дочкой GreenMDC?

– Руководители GreenMDC входят в число учредителей компании «Циф-

ровой остров», но юридически мы независимы и не обязаны поставлять модульные ЦОДы именно этого производителя. Все зависит от пожеланий заказчика и его конкретных технических требований.

– Каковы конкурентные преимущества вашего сервиса?

– В настоящее время никто в России не предоставляет ЦОД как сервис на площадке клиента. У вендоров и интеграторов были такие попытки, но их бизнес-модели не позволяли предложить конкурентную цену по сравнению со строительством заказчиком собственного корпоративного data-центра, да и срок аренды был достаточно большим – от трех лет.

К тому же бизнес-модель предусматривала сдачу в аренду только вновь произведенных ЦОДов, что сильно увеличивало срок развертывания инфраструктуры и негативно влияло на цену. У нас же в наличии есть готовые модульные ЦОДы в популярных конфигурациях.

Наша компания тщательно проработала ценообразование с учетом издержек производства, обслуживания и срока возврата инвестиций. В итоге получилось немного дороже, чем размещение в коммерческом ЦОДе по модели colocation, однако коммерческие data-центры и облачные провайдеры не являются нашими конкурентами, так как в их случае данные передаются за пределы компании.

В отличие от строительства своего data-центра модель DCaaS не требует непрофильной экспертизы, обеспечивает гибкость, экономит время и затраты на обслуживание. Существенный фактор – data-центры есть в наличии и могут быть быстро установлены у заказчика. Находящиеся на складе модульные ЦОДы мощностью 24 и 40 кВт – в течение 20–30 рабочих дней в зависимости от места размещения.

Есть вариант договора, включающий выкуп data-центра через три года эксплуатации за месячный платеж.

– ЦОД поставляется с ИТ-оборудованием?

– «Цифровой остров» прежде всего ориентируется на конструктив ЦОДа и инженерную инфраструктуру: электропитание, охлаждение, СКС. Но у компании есть партнеры, что позволяет поставлять ЦОДы с ИТ-оборудованием. Кроме того, в сотрудничестве с ними разрабатываются программно-аппаратные комплексы (ПАК), включающие инженерное и активное оборудование. Такие ЦОДы, как правило, создаются для специализированных задач, например, ЦОД для ИИ.

В подобных случаях заказчику не надо думать об интеграции прикладных программ, операционных систем и инженерного оборудования, все собрано и подогнано заранее. Например, в ЦОДах для ИИ используются высоконагруженные стойки с тщательно подобранный системой охлаждения.

В России такие ПАКи еще не предлагаются, но за рубежом уже используют.

– Какие этапы надо пройти, чтобы получить сервис по модели DCaaS?

– Прежде всего определяем модель и мощность ЦОДа. Поскольку ЦОД модульный, мы можем как расширить проект на модуль, имеющийся на складе, так и изготовить новый. Затем подписываем договор, в котором фиксируются стоимость, срок аренды, виды обслуживания, доступ к мониторингу и SLA. После проведения авансового платежа приступаем к производству недостающих модулей будущего ЦОДа и подготовке площадки для установки. После доставки и подключения к инженерным сетям запускаем ЦОД и инструктируем персонал арендатора. Затем на протяжении всего срока аренды обеспечиваем сервисное обслуживание. Причем стоимость сервисного обслуживания входит в стоимость аренды.

– Как осуществляется мониторинг ЦОДа?

– В настоящее время пользуемся Центром мониторинга компании GreenMDC, который получает информацию от ЦОДов в круглосуточном режиме. При возникновении нештатных или аварийных ситуаций оповещаются специалисты и заказчик. Ряд превентивных мер можно принять удаленно. Остальное – работа местных партнеров, которые обслуживают модульные ЦОДы «Цифрового острова» и GreenMDC по всей России. Это разные компании и разные специалисты, но каждый из них прошел обучение, сертификацию и им можно доверить обслуживание.

– Как быстро приезжает специалист?

– В зависимости от контракта есть разные варианты обслуживания, в том числе приезд специалиста за 24 часа в самый отдаленный уголок России. В Москве специалист может приехать в течение часа. Это зависит от договора и места расположения клиента. Но, как показал 12-летний опыт мониторинга и обслуживания МЦОДов, в столь быстрой реакции нет необходимости,

поскольку все критичное оборудование зарезервировано. И нет необходимости срочного вмешательства в его работу – автоматика все сделает сама.

– Как проверяется качество продукции?

– Мы уверены в надежности данных-центров, так как уделяем большое внимание выбору и тестированию оборудования. Компания покупает prefab-ЦОДы, т.е. предварительно собранные на заводе. Перед отгрузкой обязываем производителя проводить заводские испытания при контроле наших инженеров. Тестирование проводится и после развертывания ЦОДа. Поддерживать качество помогает и регламентное техобслуживание.

– Как обеспечивается безопасность? Есть ли доступ к системам безопасности ЦОДа у клиентов?

– В данных-центре установлены системы безопасности, включающие датчики открытия и закрытия, взлома, внешние и внутренние камеры видеонаблюдения с хранением записей, систему контроля и управления доступом. Мониторинг может осуществляться не только на стороне Центра мониторинга компании, но и на стороне заказчика. Системы безопасности ЦОДа при необходимости могут быть интегрированы в системы заказчика.

– Как обстоит дело с импортозамещением? Какова степень локализации ваших ЦОДов?

– Степень локализации высокая. Если провести аналогию с критериями Минпромторга, то больше 40%. Можем достичь уровня 100%, но эта серия пока в разработке. Если клиенту будет нужен ЦОД уровня Tier II полностью на российском оборудовании – сделаем и такой. DCaaS поможет компаниям осуществить импортозамещение. Если речь идет о ЦОДе мощностью до 100 кВт, то проще взять в аренду интегрированный данных-центр, включающий инженерную инфраструктуру, ИТ-оборудование и российское ПО. В нем все проблемы совмещения российских программ

с «железом» решены поставщиком. Вместе с тем по требованию заказчика можем использовать оборудование конкретных зарубежных вендоров.

– Расскажите о публичных внедрениях.

– Компания работает полгода, но публичные внедрения уже есть. Это ЦОДы для московского Центра организации дорожного движения (ЦОДД). «Цифровой остров» отвечает за инженерную инфраструктуру, а программное обеспечение – в зоне ответственности заказчика.

– Каковы планы компании?

– В ближайших планах – работа над комплексными решениями, где инженерная инфраструктура ЦОДа выступает частью программно-аппаратного комплекса, решающего задачу клиента. На российском рынке уже есть компании, разрабатывающие ПАКи для конкретных задач. Наша цель шире – сделать для них инженерную часть, оптимальный ЦОД для конкретного ПАКа. Не нужно будет строить универсальный ЦОД, а потом интегрировать в него ПАК. Заказчик сразу получит интегрированное решение.

За рубежом набирает силу тренд, когда вычисления распределяются по кластерам, включающим разные инженерные структуры. Один ЦОД в компании предназначается для решения одной задачи, скажем, для ИИ, второй – для бухгалтерии, третий – для операционной деятельности, четвертый с повышенной безопасностью – для хранения особо ответственных данных. Будем стараться соответствовать тренду.

Другая задача – объяснять заказчикам преимущества модели DCaaS, дать возможность каждому создавать свою независимую ЦОД-инфраструктуру, свои «цифровые острова».

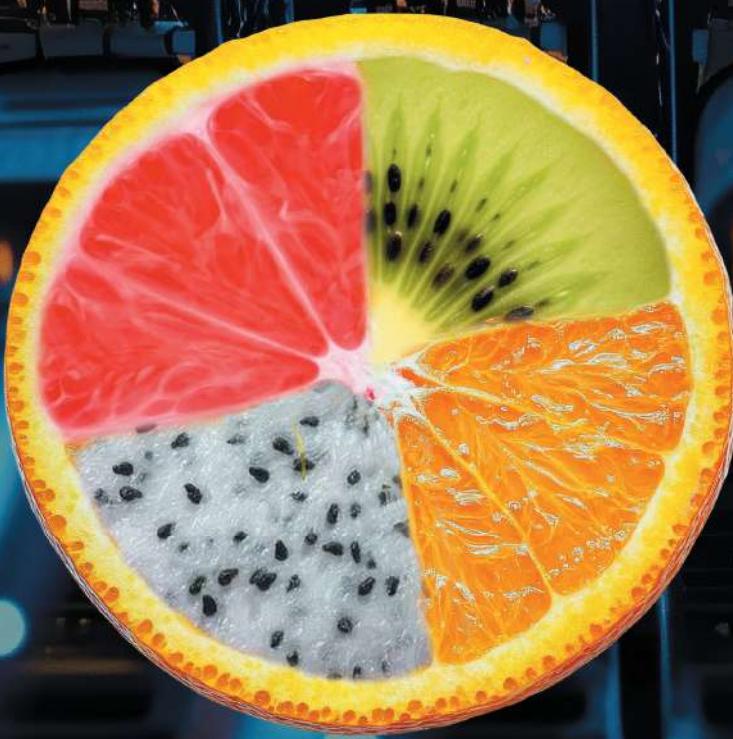


ЦИФРОВОЙ ОСТРОВ

безопасное пространство для ваших данных

d-ostrov.ru

Данные и питание по одному кабелю



Высокая востребованность разнообразных информационно-телекоммуникационных систем с централизованной схемой построения побуждает массово использовать комбинированные кабели, в сердечнике которых присутствуют и медные проводники, и волоконные световоды.



Андрей Семенов,

докт. техн. наук,
профессор, МТУСИ

Николай Кудрявцев,

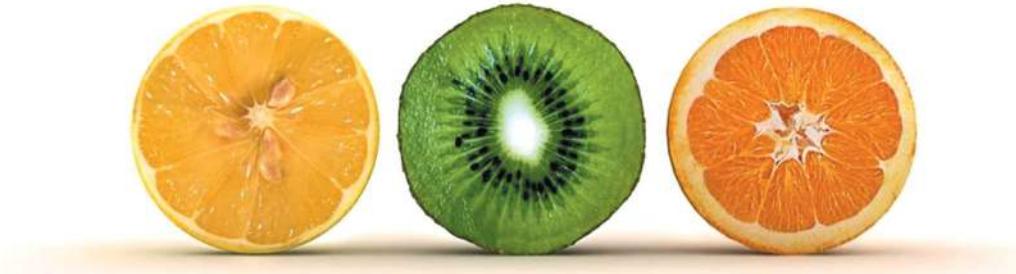
ведущий инженер,
«Гиперлайн»

Необходимость внедрения новых типов кабелей СКС

Согласно концепции, разработанной еще в 1980-х гг., СКС реализуется как иерархическая структура. Ее горизонтальная подсистема выполняется на базе кабелей из витых пар и соответствующего коммутационного оборудования, которые поддерживают передачу информации со скоростью до 10 Гбит/с на максимальное расстояние 100 м и отличаются относительно невысокой стоимостью, технологичностью монтажа и простотой эксплуатации. Они обеспечивают работоспособность различных видов сетевого терминального оборудования с потребляемой мощностью до нескольких десятков ватт без наличия местного источника. Последняя опция подразумевает использование технологии PoE.

100-метровая протяженность горизонтальных кабельных трактов была ориентирована в первую очередь на потребности ЛВС. Первые два десятка лет существования СКС как самостоятельного технического направления это вполне отвечало требованиям практики. Однако в начале 2020-х гг. ситуация радикально изменилась, поскольку широкое распространение получили различные информационные системы с выраженным тяготением к централизованной архитектуре (рис. 1). Для них 100-метровое ограничение по дальности связи – серьезный недостаток. Кроме того, терминальное оборудование таких систем сложно обеспечить дистанционным питанием по технологии PoE.

Рис. 1. Доля устройств ИТС, использующих технологию PoE, в общем объеме устройств каждой категории (по данным журнала Cabling Installation and Maintenance)



Первая из этих проблем легко решается переходом на волоконно-оптическую технику, которая поддерживает скорости вплоть до нескольких сотен гигабит в секунду на расстоянии до нескольких десятков километров. Проблема с дистанционным питанием существенно сложнее. Дело в том, что упомянутая технология PoE внедряется в ИТС методом фактического наложения на горизонтальную подсистему СКС в предположении ее реализации на симметричных кабелях. Поэтому оборудование стандартов IEEE 802.3at и IEEE 802.3bt изначально рассчитывалось на максимальное 25-омное шлейфовое сопротивление витой пары как средства доставки тока питания на приемник. Это существенно ограничивает предельную протяженность тех трактов, в которых не применяются репитеры PoE.

Известна технология PoF, обеспечивающая дистанционное питание различных терминальных устройств по волоконным световодам на расстоянии как минимум нескольких километров. Однако по волокнам стандартных оптических кабелей СКС она поддерживает максимальную мощность нагрузки не более 1–1,5 Вт, что закрывает ей путь в типовые проекты ИТС.

Остроту проблемы уменьшает то, что от вновь вводимых систем ИТС не требуется высокого быстродействия (они работают на скоростях не выше 100 Мбит/с). Это позволяет увеличить дальность связи до 150–200 м за счет применения высококатегорийных кабелей. Они отличаются увеличенным диаметром токопроводящих жил

(ТПЖ) витых пар и соответственно пониженным шлейфовым сопротивлением. Но и увеличенная в 1,5 и даже в 2 раза дальность действия часто слишком мала для современных проектов ИТС.

Базовые компоненты конструкции комбинированного кабеля

Таким образом, развитие ИТС подталкивает к широкому применению изделий новой разновидности – комбинированных кабелей (Hybrid cables, согласно терминологии ISO/TIA), в сердечнике которых присутствуют и медные проводники, и волоконные световоды. Медные проводники могут использоваться и как цепь передачи сигналов, и как средство доставки на нагрузку тока дистанционного питания, а в шнуровых кабелях – и в качестве компонента системы трассировки и интерактивного управления. Волоконные световоды поддерживают информационное взаимодействие сетевых интерфейсов, находящихся на разных концах тракта, а в шнуровых кабелях также могут быть компонентом системы трассировки и интерактивного управления.

Комбинированный кабель как функционально законченное изделие не нарушает положения стандартов СКС. Базовые нормативные документы фиксируют разрешенные типы среды передачи информационных сигналов, но не запрещают применять в сердечнике одного кабеля одновременно несколько таких сред, а также использовать одну из них не для передачи информации, а для вспомогательных технологических нужд. Последней особенностью в

своё время воспользовались разработчики оборудования PoE.

Комбинированные конструкции создавались еще на ранних этапах развития техники СКС – чтобы обеспечить скоростные характеристики, необходимые для ЛВС. Так, немецкая компания Ackermann использовала кабель с двумя волокнами и двумя витыми парами в качестве основы системного решения AMCS (all media cabling system). Разработка была ориентирована на централизованные оптические архитектуры с предельной протяженностью кабельного тракта 300 м. С ее помощью предполагалось устранить основной недостаток подобных структур в их классическом исполнении: они поддерживали только функционирование ЛВС и не обеспечивали пользователей ИТС телефонной связью. Витые пары комбинированного кабеля AMCS позволяли подключать к информационной розетке обычные телефоны, а по волоконным световодам работали сетевые интерфейсы ЛВС. Однако из-за слабой востребованности централизованных оптических архитектур концепция не получила дальнейшего развития и перестала продвигаться разработчиком уже к началу 2010-х гг.

Отдельно укажем на то, что стандарты СКС не запрещают использовать в конструкции горизонтального и магистрального кабелей дополнительные металлические и непроводящие элементы. Поэтому медные жилы могут рассматриваться только как средство подачи тока дистанционного питания на терминальное устройство, и от них не требуется соответствовать определенной категории в качестве среды передачи сигнала.

Сечение токопроводящих жил

Далее будем рассматривать медные токопроводящие жилы комбинированного кабеля только как средство доставки тока дистанционного питания источника PoE на нагрузку (т.е. на терминальное устройство ИТС, а при необходимости формирования трактов большой протяженности – на репитер PoE). Для минимизации доработок источника и приемника дистанционного питания при выборе сечения этих жил предельно допустимую величину шлейфового сопротивления примем равной 25 Ом. ТПЖ по калибру выбираем из ряда 24, 20, 16 и 12 AWG. Дальнейшее уменьшение калибра нецелесообразно из-за недопустимо большого снижения гибкости конструкции.

Максимальную протяженность кабельного тракта, реализованного на основе комбинированного кабеля, можно оценить по формуле:

$$L_{\max} = 100 \frac{S_x}{S_{24}} \times \frac{n}{2},$$

где S_x – площадь поперечного сечения ТПЖ калибром x AWG, n – количество пар ТПЖ в конструкции.

Приведенные в таблице результаты расчетов следует рассматривать как консервативную оценку (т.е. реальная дальность связи по кабелю с соответствующим калибром ТПЖ будет несколько больше указанной в таблице), поскольку они не учитывают дополнительное уменьшение длины ТПЖ из-за отсутствия укрутки, а также некоторое снижение сопротивления за счет использования в качестве реперного значения ТПЖ с диаметром 0,512 мм вместо 0,5 мм.

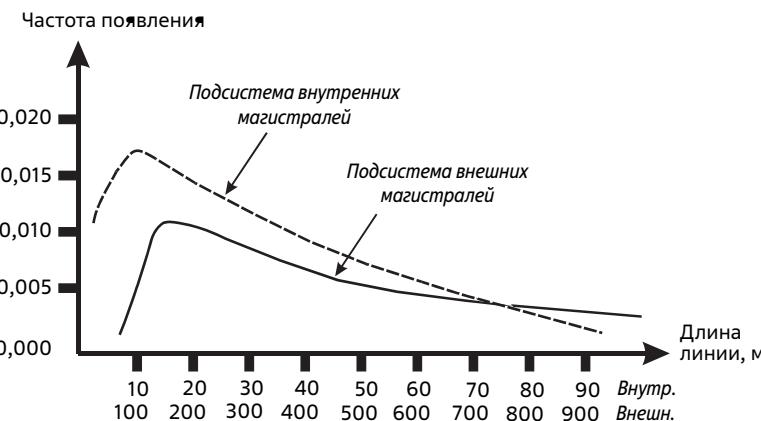


Рис. 2. Распределение длин магистральных подсистем больших СКС

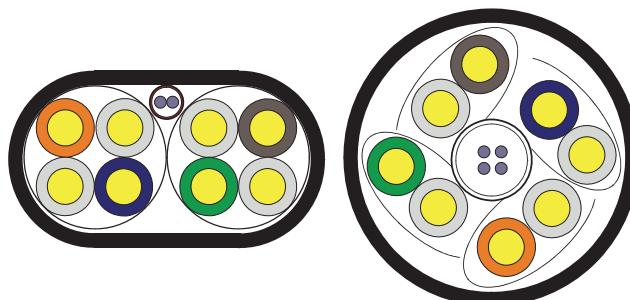


Рис. 3. Комбинированные кабели внутренней прокладки при четверочной и парной скрутке медных ТПЖ

Номенклатура комбинированных кабелей СКС

В качестве меры ожидаемых длин пробросов комбинированного кабеля с учетом его назначения и области применения целесообразно принять типовые значения протяженности стационарных линий магистральных подсистем больших (несколько тысяч портов) СКС, которые разворачиваются в нескольких зданиях на общей территории. Распределение соответствующих значений подчиняется закону, близкому к экспоненциальному (рис. 2). Отличия наблюдаются только в средних значениях длин: примерно 45 м для подсистемы внутренних магистралей и около 550 м для подсистемы внешних магистралей. С учетом столь большой разницы в ожидаемых длинах номенклатуру комбинированных кабелей логично разбить на изделия внутренней и внешней прокладки.

Калибр ТПЖ, AWG	24	20	16	12
Сечение ТПЖ, мм ²	0,205	0,518	1,31	3,31
Одна пара, м	50	126	320	807
Две пары, м	100	253	639	1612

Расчетная предельная протяженность тракта на основе комбинированного кабеля с различным калибром ТПЖ дистанционного питания

[инфраструктура]

При конструировании кабеля внутренней прокладки можно воспользоваться хорошими массогабаритными показателями волоконных световодов и интегрировать трубку с ними прямо в сердечник традиционного горизонтального кабеля. Интеграция возможна как при четверочной, так и при парной скрутке изолированных проводников (рис. 3). Недостаток такой конструкции – в сложности ее разделки при подключении к аппаратуре.

Для получения круглой в сечении формы в состав кабельного сердечника можно ввести филлеры-заполнители (рис. 5).

Обеспечение необходимой гибкости конструкции

Кабели внутриобъектовых систем часто приходится прокладывать в стесненных условиях, поэтому для них критически важна высокая гибкость. Из-за увеличенного по сравнению с типовыми горизонтальными кабе-

рабочее напряжение оборудования PoE позволяют дополнительно уменьшить толщину изоляции отдельных проводов и соответственно немного улучшить массогабаритные показатели готового кабеля.

Комбинированный кабель как компонент системного решения

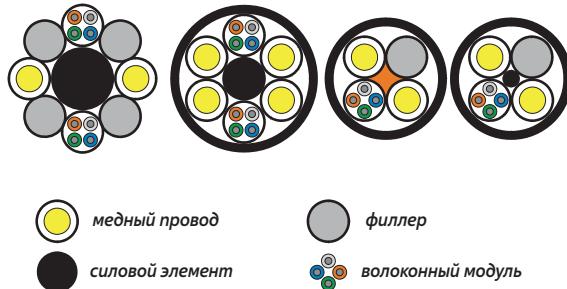
СКС того или иного производителя, как правило, представляет собой полноценное системное решение,



Рис. 4. Варианты исполнения комбинированных кабелей внутренней прокладки



Рис. 5. Варианты исполнения комбинированных кабелей внешней прокладки



Опыт эксплуатации внутриобъектовых офисных ИТС показывает, что общая оболочка волоконно-оптических кабелей внутренней прокладки (исполнение кабеля по схеме *heavy duty*) на практике применяется просто как удерживающее покрытие при необходимости сохранить структуру сердечника. Промышленность учитывает этот момент и предлагает достаточно широкую номенклатуру серийных безоболочечных конструкций (рис. 4). Отсутствие у них круговой симметрии не считается серьезным недостатком из-за небольших длин организуемых стационарных линий.

Изделиям для внешней прокладки необходима дополнительная защита от влаги, для чего используется внешняя оболочка. Ее наличие заставляет применять модульные конструкции.

лями сечения ТПЖ для получения необходимых изгибных параметров нужны дополнительные технические приемы.

Первый из таких приемов очевиден: отказаться от жесткой монолитной токопроводящей жилы в пользу многопроволочной. Второй прием заключается в уменьшении диаметра отдельной ТПЖ и увеличении количества таких проводников для обеспечения необходимого общего поперечного сечения. Чтобы устранить нежелательную «рыхлость» кабельного сердечника, отдельные провода дополнительно скручиваются в пару.

Отметим, что отсутствие необходимости поддерживать 100-омное волновое сопротивление и малое

которое позволяет выполнять определенный класс задач без привлечения дополнительного оборудования. Данный принцип целесообразно распространить и на комбинированные кабели.

С практической точки зрения это означает необходимость расширить номенклатуру поставляемой элементной базы на источники питания и соответствующие приемники. Полезно также ввести в состав каталожного предложения влагозащищенные корпуса с возможностью подогрева – для установки телекамер, точек доступа Wi-Fi и иного аналогичного оборудования. При вхождении в состав системного решения привлекательность комбинированного кабеля для конечного пользователя существенно повышается. **ИКС**



ALCON DC NORD
TECHPARK

ИННОВАЦИОННЫЙ ЦЕНТР «ТЕХНОПАРК «АЛКОН СЕВЕР»

ЦДО TIER IV

21 МВт

2

серверные MDA и основные
комнаты ввода

3 кв 2026 года

ввод в эксплуатацию

5 кВт

средневзвешенная
плотность мощности
на одно стойко-место

12

машинных залов

всего 1960 стойко-мест



Москва, САО,
Балтийский 3-й пер., вл. 5
+7 (495) 967-69-23
apanin@alcongroup.ru

Реклама

VSP Global: от проектировщика к ЦОД-девелоперу

На российском рынке не так много команд, предоставляющих комплексные услуги проектирования и построения ЦОДов. Одна из них – VSP Global. С компанией знакомит ее учредитель и генеральный директор Александр Овчинников.



– Александр, расскажите о своем опыте работы на рынке проектирования и строительства ЦОДов. Когда на этот рынок вышла VSP Global?

– Я начал заниматься ЦОДами еще в 2011 г. Компания, в которой я тогда работал, проектировала ряд крупных, знаковых объектов, в том числе ЦОД Сбербанка РФ. После участия в таких серьезных проектах тематика ЦОДов увлекла. Начал учиться, окончил курсы Uptime Institute, получил сертификат Accredited Tier Designer.

В 2018 г. в качестве партнера подключился к своему другу в компании VSP Global. Эта компания была создана в 2012 г. и специализировалась на небольших работах, связанных в основном с архитектурно-строительным проектированием. Моя инженерная экспертиза и опыт существенно расширили компетенции компании, открыли дорогу новым проектам.

VSP расшифровывается как «Васту Структура Проектирования». Васту –

это традиционная индуистская система архитектурного планирования и дизайна, и в соответствии с принципами Васту компания реализовала несколько объектов, в основном жилых. Это отдельная большая тема для беседы.

– Чем для вас привлекателен рынок цдостроения?

– Уже два десятилетия рынок ЦОДов устойчиво растет, причем довольно высокими темпами. Несмотря на все сложности и кризисы, не было ни одного провального года. Трудно найти другие рынки, которые развиваются столь же стабильно.

И в обозримой перспективе рост продолжится. Связано это с очевидной тенденцией непрерывного увеличения объема хранимых и обрабатываемых данных. Чтобы подтвердить этот тезис, я обычно спрашиваю у людей, как часто они чистят свои облачные хранилища информации. Многие отвечают – «никогда». Мало того,

что люди генерируют огромное количество фотографий и видеороликов, так и старая информация никуда не исчезает. Плюс стремительное развитие рынка интернета вещей, сервисов онлайн-доставки, маркетплейсов.

Еще один драйвер – искусственный интеллект. Он даст существенный импульс развитию отрасли ЦОДов. В ближайшие 10 лет многократно увеличится спрос на вычислительные мощности и соответственно на инженерную инфраструктуру для этих мощностей.

– Какова значимость (доля) сегмента ЦОДов в общем объеме бизнеса компании VSP Global?

– VSP Global много занималась проектированием жилья, общественных зданий, промышленных объектов. Сначала ЦОДы были небольшой частью бизнеса, не более 30%. Но в 2020–2021 гг. запрос на проектирование ЦОДов начал резко расти. Предложения буквально посыпа-

лись. Только за прошлый год через нас прошли пять проектов крупных дата-центров – это рекорд за все годы моей работы в цдовской индустрии. А всего за последние пять лет VSP Global участвовала в проектах дата-центров общей емкостью 15,5 тыс. стойко-мест и более 100 МВт ИТ-мощности.

Замечу, что начиная с середины 2010-х гг. был период, когда на рынке цдостроения доминировали классические системные интеграторы. Они брали на себя и проектирование, и поставку оборудования, и строительство – короче говоря, контракты под ключ. А поскольку стоимость собственно проектирования составляет лишь около 1% стоимости проекта ЦОДа, то они раскладывали этот процент на стоимость оборудования, на строительство и выполняли проектирование существенно ниже себестоимости. Скажем, при стоимости проектирования 50 млн руб. делали проект за 1 млн руб. Поэтому «чистым» проектировщикам, которые не занимались поставкой оборудования, было сложно конкурировать с такими интеграторами.

Сейчас ситуация кардинально изменилась. Дело в том, что системные интеграторы обычно работают с определенными вендорами и зачастую практически навязывают заказчику технические решения «своих» вендоров. А эти решения могут оказаться неоптимальными для конкретных проектов. Поэтому интерес к независимому (от вендоров) проектированию вырос.

– Так ваши компетенции – только проектирование?

– Начинали с проектирования. Но в широком смысле этого слова, включая сюда разработку концепции, проведение изысканий, формирование рабочей документации. Работаем со сметной документацией. Ведь при разработке технических решений проектировщик должен предложить оптимальный по стоимости вариант без снижения надежности. В нашей команде 40 проектировщиков, у большинства есть опыт проектирования в области ЦОДов.

В 2024 г. в нашей деятельности произошли знаковые изменения: мы в качестве генерального подрядчика начали строить в Москве центр обработки данных общей мощностью 50 МВт. В дальнейшем планируем реализацию проектов под ключ, от концепции до ввода в эксплуатацию. Стремимся стать ЦОД-девелопером.

В следующих выпусках я подробнее расскажу об объекте и о ходе его строительства.

– Что вы считаете основным препятствием на пути развития отрасли ЦОДов в России?

– Наверное, не буду оригинал, если скажу, что сегодня самый главный тормоз – это высокая стоимость денег. С оборудованием больших проблем нет. Имею в виду инженерные системы. Не буду говорить про ИТ-оборудование (серверы, СХД), поскольку ЦОД – это все-таки инженерная инфраструктура, платформа для развертывания ИТ-систем. Появилось много неплохого импортозамещенного оборудования. После введения санкций и ухода с рынка большинства европейских и американских вендоров российские производители окрепли и стали уверенно чувствовать себя на рынке. Кроме того, доступны продукты из Китая и других дружественных стран. Недавно вернулся из КНР и могу подтвердить: все, что необходимо для ЦОДа, можно закупить в Поднебесной.

– Вы говорили, что многие системные интеграторы привязаны к конкретным производителям. А как VSP Global строит работу с производителями?

– Как проектную организацию нас всегда отличала гибкость. Мы позиционируем себя как открытую компанию, которая работает в интересах заказчика, делает то, что нужно заказчику. Поэтому мы не привязываемся к определенным вендорам.

Но в силу специфики цдовских проектов на рынке не так много компаний-вендоров, которые предо-

ставляют подходящее оборудование. По критическим системам, таким как бесперебойное и гарантированное электропитание, охлаждение, мы ориентируемся на основных вендоров. Как правило, это три-четыре компании. Для нас важно, чтобы производитель уже имел опыт работы с ЦОДами, положительные отзывы от других заказчиков – операторов и владельцев ЦОДов. В идеальном случае желательно, чтобы оборудование вендора применялось в ЦОДах лет десять, имелась определенная статистика отказов и т.д.

– Каковые ваши планы дальнейшего развития на рынке цдостроения?

– Прорабатываем собственный проект ЦОДа, привлекаем под него инвестиции. Даже есть планы не просто построить ЦОД, в который можно установить высоконагруженные стойки, а наполнить эти стойки ИТ-оборудованием и предоставлять инфраструктуру для систем на основе искусственного интеллекта. Другими словами, стать сервис-провайдером, например, предложить услуги GPUaaS.

Но это долгосрочная перспектива. А ближайшая, как я уже говорил, – стать ЦОД-девелопером. Чтобы выйти на полный цикл в области цдостроения, осваиваем новые возможности. Например, некоторые наши проекты уже успешно прошли сертификацию в Uptime Institute проектной документации (Design), построенного объекта (Facility) и эксплуатации (Operations). Скоро сможем сертифицировать согласно Constructed Facility объект, построенный собственными силами. Короче говоря, мы готовы брать проект на стадии концепции и делать все до ввода ЦОДа в эксплуатацию. И руководствоваться принципом открытости: не навязывать решения, а подбирать оптимальные по надежности, качеству, стоимости.



vspglobal.ru

Построение системы энерgosнабжения крупных ЦОДов на базе газовой генерации

Михаил Котляров,

технический директор,
«ДиСиСи» (DCC)

Виталий Чумаченко,

заместитель генерального
директора по моделированию
энергосистем,
«Неорганические сорбенты»,
канд. техн. наук

Сергей Паскевич,

начальник отдела
тарифообразования в ТЭК,
«Ситэкс», канд. экон. наук

**Энерgosнабжение ЦОДа должно быть
надежным, экономически эффективным и
экологичным. Поэтому сегодня все большее
внимание привлекает возможность
использования газовой генерации.**

Первым делом – надежность

Для классификации и оценки надежности ЦОДов и доступности предоставляемых на их базе сервисов в мире широко используется система стандартов, разработанная Uptime Institute. На основе конкретных требований к архитектуре и инфраструктуре ЦОДа стандарты Tier определяют уровни надежности, оценивая возможности данных центров с точки зрения времени безотказной работы. Соответственно этому выдвигаются требования к источникам энерgosнабжения (табл. 1).

Основное и принципиальное различие между Tier III и Tier IV в том, что

топология построения инженерной инфраструктуры Tier III позволяет проводить плановое обслуживание систем и любых компонентов без прерывания работы ЦОДа, а уровень надежности Tier IV подразумевает работоспособность ЦОДа при любом единичном отказе в любой точке инженерной инфраструктуры или проведении любых мероприятий по обслуживанию систем.

В соответствии с Правилами устройства электроустановок (ПУЭ), утвержденными Приказом Минэнерго России от 08.07.2002 № 204, приемники электрической энергии по надежности энерgosнабжения разделяются

на несколько категорий. Категория определяется в первую очередь рисками, которые могут возникнуть при перерыве энерgosнабжения. Согласно п. 1.2.18 ПУЭ, к электроприемникам первой категории относятся электроприемники, перерыв энерgosнабжения которых может повлечь за собой опасность для жизни людей, угрозу для безопасности государства, значительный материальный ущерб, расстройство сложного технологического процесса, нарушение функционирования особо важных элементов коммунального хозяйства, объектов связи и телевидения. Из состава электроприемников первой категории выделяется особая группа

Табл. 1. Требования
к энерgosнабжению
ЦОДов различных
уровней надежности

Показатель	Tier I	Tier II	Tier III	Tier IV
Резервирование оборудования	N	N + 1	N + 1	2N
Распределенные потоки	1	1	2	2
Обслуживание ЦОДа без остановки	Нет	Нет	Да	Да
Отказоустойчивость	Нет	Нет	Нет	Да



электроприемников, бесперебойная работа которых необходима для безаварийного останова производства с целью предотвращения угрозы жизни людей, взрывов и пожаров.

В ЦОДе зачастую даже кратковременное отключение электропитания приводит к простою сервисов клиентов, потере данных критически важных приложений, значительным финансовым потерям и серьезным репутационным рискам. Исходя из этого может сложиться мнение, что ЦОДы уровня Tier III соответствуют первой категории, а ЦОДы уровня Tier IV – первой особой категории. Однако это не так.

Согласно Uptime Institute Tier Standard: Topology (п. 2.5), перебои в электрической сети (внешней) считаются не аварийной ситуацией, а ожидаемым рабочим условием, к которому площадка полностью подготовлена. Дело в том, что комплекс стандартов Uptime Institute описывает архитектуру всей системы энергоснабжения ЦОДа, в то время как в ПУЭ рассматривается только точка подключения к электрической сети.

Откуда ЦОДу брать электричество

Из стандартов Uptime Institute следует, что ЦОД Tier III и Tier IV – это отдельный энергопотребитель, обязаный иметь собственный источник генерации электрической энергии, который не зависит от внешних условий и среды и к которому как к части инженерной инфраструктуры предъявляются такие же требования по уровню надежности (ЦОДы Tier I и II также должны иметь собствен-

ные источники генерации, однако требования к уровню их резервирования ниже. – Прим. ред.). При этом подключение к внешнему источнику энергоснабжения рассматривается скорее как альтернатива, обеспечивающая экономию ресурсов при работе площадки в нормальном режиме по сравнению с питанием ее от собственных источников. Таким образом, по требованиям к надежности энергоснабжения ЦОДы уровней Tier III и IV существенно отличаются от обычных потребителей. Эта разница обусловлена критичностью бесперебойной работы объекта.

В ЦОДах в качестве основного и гарантированного источника, как правило, рассматриваются двигатель-генераторы (система гарантированного энергоснабжения, СГЭ) в связке с источниками бесперебойного питания, которые должны или быть непрерывно в работе, или автоматически запускаться и принимать нагрузку при прекращении энергоснабжения от внешних электросетей. Помимо этого, все критическое оборудование, не запитанное от ИБП, должно автоматически запускаться после восстановления электропитания. Согласно требованиям Uptime Institute, СГЭ должна быть в состоянии работать без перебоев и иметь достаточный запас топлива на поддержание своей деятельности в течение 12 ч.

Обычно организация основного энергоснабжения небольших корпоративных data-центров не вызывает особых трудностей. Однако с развитием цифровой экономики, ростом числа электронных серви-

сов, увеличением объема хранимых и обрабатываемых данных, а также с расширением спектра электронных услуг энергопотребление data-центров также растет. В результате мощность крупных, гипермасштабных ЦОДов может достигать нескольких сотен мегаватт. Использование дизель-генераторных установок (ДГУ) в таких проектах может оказаться не самым эффективным решением. Это обусловлено необходимостью их частого обслуживания, потребностью в площадях для размещения большого количества установок, сложностями создания инфраструктуры и организации непрерывного пополнения запасов топлива (нужно обеспечить нахождение и разгрузку на площадке одновременно нескольких десятков автоцистерн).

Сравнение технологий производства электроэнергии показывает, что в качестве основной технологии для таких потребителей, как крупные ЦОДы, наиболее приемлема газовая генерация, представленная газотурбинными установками (ГТУ) или газопоршневыми агрегатами (ГПА). В пользу этого выбора говорит ряд преимуществ газовой генерации, среди которых – высокая надежность энергоснабжения, возможности следования за нагрузкой и относительно быстрый запуск по сравнению с другими источниками (табл. 2). Кроме того, ГТУ имеют более низкую удельную дисконтированную стоимость производства электроэнергии (levelized cost of energy, LCOE), чем, скажем, дизельные электростанции (ДЭС). Например, для крупного потребителя (90 МВт) LCOE составляет 14,52 руб./кВт•ч в случае ДЭС против

Преимущества	Недостатки
Обеспечение первой категории энергоснабжения даже при отсутствии связи с энергосистемой	Малая длительность работы между техническим обслуживанием
Меньшие габариты, чем у ДЭС той же мощности	Ресурс – от 100 тыс. ч
Относительно короткие сроки строительства (около трех лет)	Риски, связанные с невозможностью поставки машиностроительной отраслью требуемого количества агрегатов в срок
Низкая удельная стоимость	
Низкие удельные затраты на топливо и эксплуатацию	

Табл.2.
Преимущества
и недостатки ГТУ



Рис. 1.
Сравнение LCOE
для ГТУ и ДЭС,
руб./кВт·ч



4,18 руб./кВт·ч при использовании газотурбинных установок (рис. 1).

Что учесть при выборе ГТУ

Подход к созданию системы энергоснабжения ЦОДа на базе газовой генерации должен быть комплексным и обеспечивать надежность, эффективность, масштабируемость и экологичность проекта.

внешней сети) и смешанный (при резервировании от сети) варианты энергоснабжения. Исключительно сетевой вариант для энергоснабжения ЦОДа, сертифицируемого в соответствии с Tier III и IV, не может рассматриваться исходя из требований п. 2.5 стандарта к обязательному наличию собственной генерации.

электрических и тепловых нагрузок, а также возможность применения ко- и тригенерации.

3. Требования к резерву мощности, а именно:

- к вращающемуся резерву (мощности генерирующих агрегатов, работающих в недогруженном состоянии в постоянной готовности принять возникающий небаланс, в том числе при отключении одного или более агрегатов);
- «холодному» резерву (мощности генерирующих агрегатов, которые требуют для своего пуска и приема нагрузки нескольких часов);
- резерву на ремонтные работы (мощности дополнительных генерирующих агрегатов, учитывающие возможность текущих и капитальных ремонтных работ блоков).

4. Категория надежности энергоснабжения технологического объекта (ЦОДа).

5. Плановый рост нагрузки, в том числе ИТ-нагрузки и затрат мощности на охлаждение в зависимости от выбранной технологии. Несмотря на то что нагрузка основного вычислительного оборудования практически постоянна, суммарная нагрузка с учетом технологии охлаждения может быть резко переменной, что усугубляет накладываемые на энергоцентр требования по маневренности и необходимости слежения за нагрузкой.

6. Резервирование генерирующего оборудования по схеме $N + 2$, где N – количество источников электроэнергии, включенных в нормальном режиме работы. Один блок добавляется для учета ремонтной схемы и один блок – для аварийного отключения агрегата.

7. Потребление мощности на собственные нужды станции. Для парогазовых и газотурбинных установок таковое, согласно Методическим указаниям по проектированию развития энергосистем (утвержден-



Рис. 2. Факторы, определяющие выбор состава генерирующего оборудования при разработке вариантов энергоснабжения ЦОДа

При выборе количества генерирующих агрегатов и их параметров нужно учитывать целый ряд факторов (рис. 2):

1. Тип связи с энергосистемой. Возможны островной (при отсутствии

2. Вид охлаждения оборудования ЦОДа – например, система «чиллер – фанкойл» на основе парокомпрессионного цикла, адиабатическая установка или абсорбционная ходильная машина (АБХМ), – который определяет характер и графики

$$\begin{cases} P_{\Sigma \text{наг лет}} + P_{\% \text{сн}} \times P_{\text{ГТУном}} \times N_{\text{ГТУвращ лет}} < P_{\text{уст. лет}} (N_{\text{ГТУвращ лет}}) \times N_{\text{ГТУвращ лет}} \\ P_{\Sigma \text{наг зим}} + P_{\% \text{сн}} \times P_{\text{ГТУном}} \times N_{\text{ГТУвращ зим}} < P_{\text{уст. зим}} (N_{\text{ГТУвращ зим}}) \times N_{\text{ГТУвращ зим}} \\ N_{\text{ГТУ}} = \min(N_{\text{ГТУвращ зим}}, N_{\text{ГТУвращ лет}}) + N_{\text{рез}} \end{cases} \quad (1),$$

где:

ным Приказом Минэнерго России от 06.12.2022 № 1286), составляет 5%.

При разработке решений энергоснабжения необходимо планировать длительную работу агрегатов и не допускать их функционирования с мощностью меньше технологического минимума, так как в этом диапазоне мощностей агрегаты работают неустойчиво и их КПД резко снижается. При наборе мощности нагрузки до допустимой величины возможно использование дополнительных нагрузочных модулей.

Для островного варианта энергоснабжения загрузка энергогенераторов должна выбираться в соответствии с необходимостью поддержания вращающегося резерва при выходе из строя одного генератора.

В частных случаях, где остро стоят вопросы автономного энергоснабжения или обеспечения гарантированного энергоснабжения за счет собственной генерации, необходимо учитывать снижение вырабатываемой электрической мощности и рост объема потребления газа ГТУ при повышении температуры воздуха на всасывании. ГТУ работают с постоянным расходом воздуха, при повышении температуры плотность воздуха уменьшается и, следовательно, снижается мощность ГТУ.

Таким образом, количество необходимых агрегатов $N_{\text{ГТУ}}$ с учетом критических факторов можно определить с помощью неравенств (1).

$N_{\text{ГТУвращ}}$ – количество блоков, включенных в работу;

$P_{\text{уст. лет}} (N_{\text{ГТУвращ}})$ – установленная мощность одного блока ГТУ с учетом коэффициента снижения мощности газовой турбины в летнем режиме и с учетом необходимости поддержания вращающегося резерва;

$P_{\Sigma \text{наг лет}}, P_{\Sigma \text{наг зим}}$ – мощность потребления ЦОДа в летние и зимние периоды с учетом затрат на охлаждение;

$N_{\text{ГТУвращ лет}}, N_{\text{ГТУвращ зим}}$ – минимальное количество агрегатов, при котором неравенство выполняется, в летние и зимние периоды;

$P_{\% \text{сн}}$ – потребление мощности на собственные нужды, процент номинальной мощности блока;

$P_{\text{ГТУном}}$ – номинальная мощность энергогенератора для ГТУ;

$N_{\text{рез}}$ – количество агрегатов, находящихся в резерве.

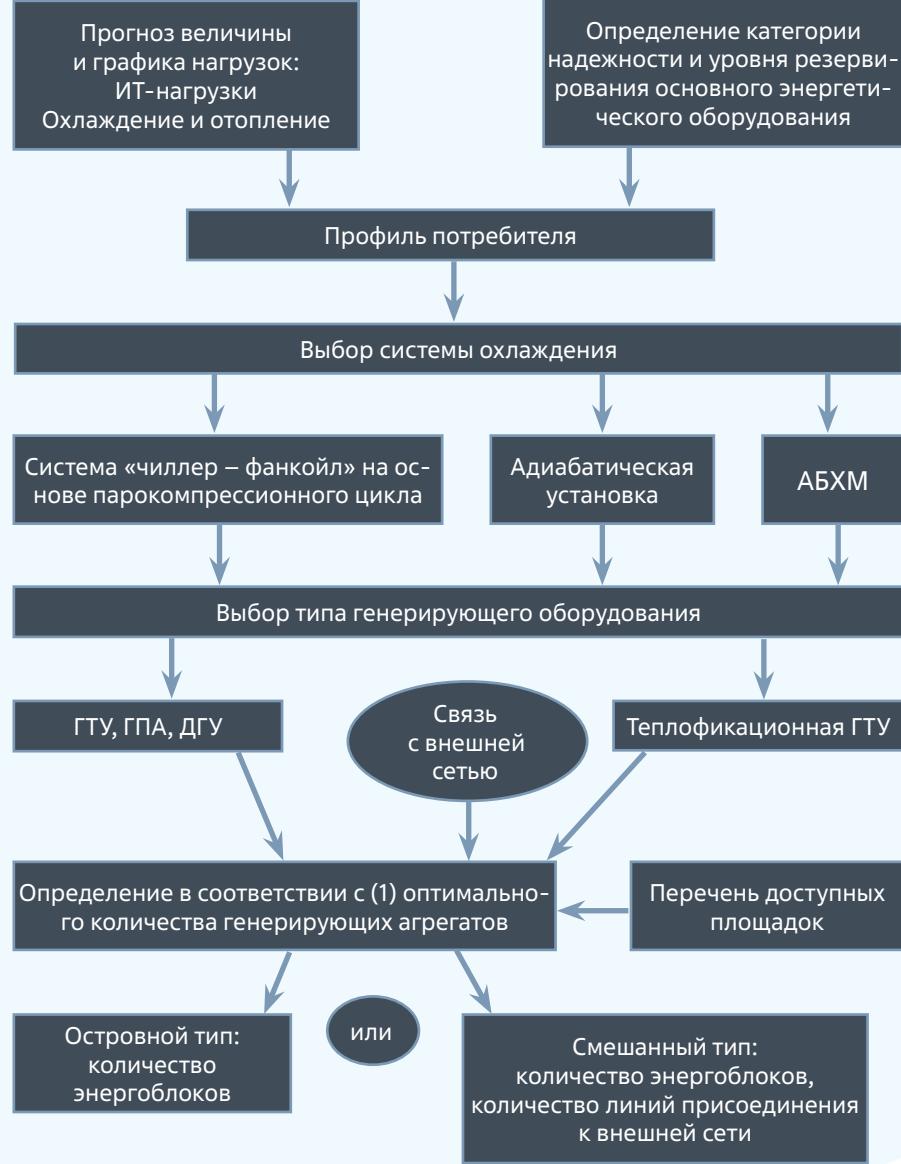


Рис. 3. Схема выбора состава генерирующего оборудования

Так, для ЦОДа уровня Tier III с планируемой потребляемой мощностью 90 МВт потребуется 11 блоков ГТУ мощностью 12 МВт; суммарная установленная мощность составит 132 МВт.

$$R_n = \frac{\sum_i^n C_n}{C_n} \quad (2),$$

где:

n – номер площадки;

R_n – ранг n -ной площадки;

C_n – средневзвешенный показатель доступности инфраструктуры для площадки n , определяемый по формуле:

$$C_n = K_{газ} \times P_{газ}^n + K_{эл} \times P_{эл}^n + K_{тр} \times P_{тр}^n + K_{межд} \times P_{межд}^n,$$

где:

$K_{газ}$, $K_{эл}$, $K_{тр}$, $K_{межд}$ – весовые коэффициенты доступности инфраструктурных объектов (газоснабжения, электросетей и транспорта, в том числе международного, соответственно);

$P_{газ}^n$, $P_{эл}^n$, $P_{тр}^n$, $P_{межд}^n$ – расстояния от n -ной площадки до объектов газоснабжения, электросетей и транспорта, в том числе международного, соответственно.

Опыт реализации проектов строительства дата-центров различной мощности и расположения позволил авторам сформулировать унифицированные подходы к разработке вариантов энергоснабжения этих объектов и выбору состава генерирующего оборудования (рис. 3), обеспечивающие соответствие международным стандартам надежности.

Где строить?

Подбор площадки для строительства ЦОДа обычно происходит в два этапа:

1. Определяется приоритетный район размещения площадки в границах региона с учетом наличия необходимой свободной площади для строительства.
2. Составляется матрица вариантов, из которой на основании ранжирования в соответствии с описанными ниже критериями методом конкурентного сравнения и анализа риск-факторов выбирается конкретный земельный участок.

Критерии выбора площадки для размещения ЦОДа:

- Доступность возможных точек присоединения к единой системе газоснабжения ($K_{газ}$), которая отражает возможность использования природного газа при минимизации затрат на его транспортировку по газопроводу-отводу.
- Доступность точек присоединения к внешней электросети ($K_{эл}$), которая отражает возможность технологического присоединения к внешней сети для смешанного варианта с целью выбора схемы резервирования энергоснабжения.

■ Доступность транспортной инфраструктуры ($K_{тр}$), которая влияет на удобство доставки обслуживающего персонала в период эксплуатации и на стоимость доставки оборудования и материалов в период строительства, а также на эксплуатационные затраты при доставке оборудования и запасных частей.

■ Доступность площадки для международного транспорта ($K_{межд}$), которая характеризует затраты на привлечение строительно-монтажного и эксплуатирующего персонала и влияет на удобство доставки персонала и конкурентную привлекательность ЦОДа для будущих пользователей и/или арендаторов.

Ранжирование потенциальных площадок проводится по формуле (2) в соответствии с присвоенными весовыми коэффициентами.



Разработанный авторами алгоритм выбора состава генерирующего оборудования, учитывающий такие факторы, как уровень надежности, связь с внешней сетью, вид охлаждения, требования к резерву мощности, может применяться при проектировании схем энергоснабжения ЦОДа любой мощности.

При рассмотрении вопросов экономической эффективности следует учитывать положения местных нормативных правовых актов, касающиеся условий нераспространения требования реализовывать всю генерируемую на таком объекте (или его части) электрическую энергию (мощность) на оптовом рынке (для России – п. 5 ст. 36 закона «Об электроэнергетике» от 26.03.2003 № 35-ФЗ).

При размещении ЦОДа в регионах с более холодным климатом совокупного эффекта можно достичь за счет экономии топлива в случае выбора системы охлаждения с использованием фрикулинга и благодаря меньшему снижению мощности ГТУ в летний период. **ИКС**



Почему будущее СХД за IP-протоколами

Илья Борняков,
генеральный директор, ITPOD

Эволюция сетевых технологий изменила требования к инфраструктуре хранения данных, поэтому IP-сети сегодня стали более перспективным решением, чем Fibre Channel, и переход на IP-протоколы положительно влияет на экономику и технологическую независимость предприятий.

В начале 2000-х годов выбор Fibre Channel для систем хранения данных был очевиден: нестабильные IP-сети с потерями пакетов и высокими задержками не могли обеспечить необходимый уровень производительности и надежности. FC-инфраструктура решала эти проблемы, предоставляя выделенную сеть с гарантированной пропускной способностью. Однако за последние 20 лет ситуация кардинально изменилась. Появление All-Flash-массивов и NVMe-накопителей трансформировало требования к СХД. Традиционные проблемы производительности отошли на второй план, а ключевыми факторами стали гибкость инфраструктуры, простота масштабирования и технологическая независимость.

Эволюция технологий СХД

В конце 1990-х — начале 2000-х годов ИТ-инфраструктура столкнулась с серьезными вызовами. Растущие объемы данных и требования к их доступности показали, что возможности существовавших тогда IP-сетей ограничены: потери пакетов, непредсказуемые задержки и сложности с обеспечением качества обслуживания (QoS) делали их неподходящими для систем хра-

нения данных критически важных приложений.

Протокол Fibre Channel появился как специализированное решение этих проблем. Он предлагал выделенную сеть для СХД с гарантированной производительностью, низкими задержками и встроенными механизмами контроля ошибок. В те годы эти преимущества полностью оправдывали высокую стоимость FC-инфраструктуры и необходимость в специализированном оборудовании.

Но технологии не стоят на месте. За последние 20 лет сети Ethernet прошли огромный путь развития:

- пропускная способность выросла с 1 Гбит/с до 100 Гбит/с и более;
- появились механизмы управления потоками и приоритизации трафика;
- кардинально улучшились алгоритмы обработки ошибок;
- снизилась стоимость оборудования при повышении его надежности.

Одновременно с этим изменились и сами системы хранения данных. Массовый переход на твердотельные накопители (SSD) и появление NVMe-интерфейса создали новую реальность, где традиционные

преимущества Fibre Channel стали неактуальны.

Во-первых, огромная пропускная способность современных IP-сетей с запасом покрывает потребности даже самых требовательных All-Flash-массивов.

Во-вторых, высокая производительность и низкие задержки NVMe-накопителей сделали избыточными многие механизмы оптимизации FC. А развитие протокола NVMe over TCP позволило эффективно использовать NVMe-накопители в стандартных IP-сетях без потери производительности.

В результате Fibre Channel из технологического прорыва превратился сегодня в наследие прошлого, которое создает проблем больше, чем решает. Необходимость поддерживать отдельную сеть, зависимость от ограниченного числа вендоров и высокая совокупная стоимость владения (TCO) делают его все менее привлекательным для новых внедрений.

Современные IP-сети с протоколом NVMe over TCP не просто достигли уровня FC по производительности и надежности — они предлагают более гибкую, экономичную и перспективную альтернативу. При этом они позволяют использовать существующую сетевую инфраструктуру и оборудование широкого круга производителей, включая российских.

Современные реалии

Проблемы с производительностью, которые определяли архитектурные решения 10 лет назад, в значительной степени преодолены: сегодня, в эпоху дата-центров, работающих с All-Flash-массивами, пропускная способность и количество операций ввода-вывода в секунду (IOPS) больше не являются ограничивающими факторами, а стремление к снижению задержек транспортной сети стало общепринятым.

На этом фоне использование Fibre Channel все чаще вызывает вопросы. Традиционные аргументы в его пользу теряют актуальность.

➔ **Надежность и отказоустойчивость.** Раньше считалось, что выделенная сеть FC обеспечивает более высокую надежность. Однако поддержка двух разных сетевых инфраструктур — FC для хранения и Ethernet для остального трафика — создает дополнительные сложности в администрировании и повышает риск ошибок. Современные IP-сети с правильно настроенной архитектурой обеспечивают необходимый уровень надежности в рамках единой инфраструктуры.

➔ **Механизмы обеспечения качества обслуживания.** Существовало мнение, что для критически важных систем хранения необходима поддержка Lossless Ethernet с комплексом технологий Data Center Bridging, Priority Flow Control и других механизмов QoS. Практика показала, что в современных условиях избыточная пропускная способность сетей устраниет необходимость в сложных механизмах приоритизации, а производительность часто оказывается выше при отключенных механизмах QoS. Кроме того, сложность настройки и поддержки этих механизмов не окупается получаемыми преимуществами.

➔ **Поддержка современных протоколов.** FC ограничен поддержкой только блочного доступа, в то время как современные системы хранения все чаще требуют поддержки файловых и объектных протоколов. IP-сети обеспечивают универсальную среду для всех типов доступа к данным.

➔ **Технологическая независимость.** Критически важной стала возможность импортозамещения. FC-оборудование производится только двумя американскими вендорами, в то время как Ethernet-коммутаторы выпускаются множеством производителей, включая российских. Например, коммутаторы от Eltex, Qtech и YADRO включены в реестр телекоммуникационного оборудования российского происхождения (ТОРП) Минпромторга, а недавно этот список пополнился сетевым оборудованием компании «Аквариус».

➔ **Простота внедрения.** NVMe over TCP обеспечивает совместимость с существующей сетевой инфраструктурой и устраниет необходимость в специализированном оборудовании. Это важно как для новых проектов, где можно сразу выбрать оптимальное решение, так и для модернизации существующих систем с постепенным отказом от FC и для построения гибридных инфраструктур в переходный период.

В результате мы видим, что продолжение использования FC в новых проектах все чаще становится данью традиции, а не результатом взвешенного технического решения. Современные IP-сети с поддержкой NVMe over TCP предлагают более перспективный путь развития инфраструктуры хранения данных.

Экономическое обоснование перехода на IP

Экономическая эффективность — один из ключевых факторов при выборе технологий сетей хранения данных. Сравнительный анализ Fibre Channel и IP-решений показывает существенную разницу в TCO.

Стоимость сетевого оборудования

Сравним типовые компоненты: двухпортовый адаптер Fibre Channel (LPe35002-M2, 32Gb) стоит примерно 140 тыс. руб., а двухпортовый Ethernet-адаптер (E810-CQDA2, 100Gb) — около 70 тыс. руб.

При этом разница в производительности впечатляет: FC-адаптер обе-

спечивает суммарную пропускную способность 64 Гбит/с, а Ethernet-адаптер предоставляет 200 Гбит/с.

Если пересчитать стоимость оборудования на единицу пропускной способности, разница станет еще более драматической. Обеспечение полосы в 96 Гбит/с с помощью FC-решения обойдется примерно в 210 тыс. руб., а с помощью Ethernet-решения — около 35 тыс. руб.

Инфраструктурные затраты

Переход на IP-протоколы позволяет снизить инфраструктурные расходы.

Во-первых, ненужность отдельной сети для СХД подразумевает исключение затрат на FC-коммутаторы и сокращение расходов на кабельную инфраструктуру, уменьшает количество точек отказа.

Во-вторых, унификация оборудования дает возможность использовать стандартные Ethernet-коммутаторы, выбирать решения от разных производителей и снизить затраты на обучение персонала.

Наконец, свой вклад в общее снижение инфраструктурных расходов вносят более высокая плотность портов в Ethernet-коммутаторах, эффективное использование пропускной способности и гибкое распределение ресурсов между разными типами трафика.

Операционные расходы

Существенная экономия достигается и на операционных расходах. За счет управления единой сетевой инфраструктурой вместо двух отдельных, уменьшения времени на ее обслуживание и упрощения мониторинга и диагностики снижаются затраты на администрирование.

Дешевле обходится обучение персонала, поскольку можно использовать имеющиеся у сотрудников компетенции по IP-сетям и не нужно проводить специальную сертификацию по FC. Кроме того, рынок труда предоставляет более широкий выбор специалистов.

Доступность технической поддержки от российских производителей и

регулярные обновления программного обеспечения уменьшают и эти статьи расходов. К тому же цикл обновления оборудования становится предсказуемым.

Перспективы развития

Инвестиции в IP-инфраструктуру более перспективны с точки зрения развития.

Масштабирование не представляет проблемы. IP-сети обеспечивают простое наращивание емкости и производительности, гибкое добавление новых узлов и сервисов, а также поддержку современных архитектур и протоколов.

Благодаря широкому выбору поставщиков оборудования и особенно наличию российских производителей значительно повышается технологическая независимость IP-инфраструктуры, не говоря уже о ее устойчивости к санкционным рискам.

Расчеты показывают, что в перспективе трех лет переход на IP-протоколы позволяет снизить совокупную стоимость владения инфраструктурой хранения данных на 40–60%. При этом важно отметить, что экономический эффект достигается не только за счет прямого сокращения затрат на оборудование, но и благодаря оптимизации операционных расходов и снижению рисков.

Импортозамещение как драйвер перемен

В условиях санкционных ограничений вопрос технологического суверенитета приобрел особую актуальность. В области систем хранения данных проблема оказалась особенно острой для инфраструктур на базе Fibre Channel.

Монополия на рынке FC

Как уже говорилось, рынок FC-решений фактически контролируется двумя американскими компаниями. Это создает критическую зависимость по нескольким направлениям:

- производство FC-коммутаторов;
- разработка и обновление прошивок;

- техническая поддержка;
- поставка запасных частей.

При этом даже китайские производители не предлагают альтернативных решений для FC-инфраструктуры. Это делает задачу импортозамещения в данном сегменте практически нерешаемой в обозримой перспективе.

Ethernet – путь к независимости

В отличие от FC-инфраструктуры на рынке Ethernet-решений выбор производителей и продуктов гораздо шире. Среди российских компаний, выпускающих коммутаторы для данных центров, можно выделить Eltex с линейкой MES5500, Qtech с серией QSW и YADRO с коммутаторами Kornfeld. Все оборудование этих компаний включено в реестр ТОРП, сертифицировано Минпромторгом и совместимо с отечественными операционными системами.

Экосистема решений

Переход на IP-протоколы открывает доступ к широкой экосистеме совместимых решений. Сетевые карты с поддержкой RDMA, серверы на базе процессоров «Эльбрус» и «Байкал» и серверное оборудование российской сборки создают гибкую и независимую основу. В области программного обеспечения IP-экосистема поддерживает отечественные операционные системы, системы виртуализации, средства мониторинга и управления, а также решения для программно

определеных хранилищ и систем резервного копирования. На базе СХД с поддержкой NVMe over TCP создается высокопроизводительная и безопасная среда для хранения и обработки данных.



Переход от Fibre Channel к IP-протоколам в системах хранения данных отражает фундаментальные изменения в подходах к построению ИТ-инфраструктуры.

Сегодня мы видим, что условия для этого перехода складываются благодаря сочетанию значительного роста производительности и надежности IP-сетей, кратного снижения стоимости оборудования при увеличении пропускной способности и разработки эффективных протоколов для работы с современными накопителями. Кроме того, на рынке широко представлено оборудование от российских производителей, совместимое с отечественными ОС.

Главным препятствием к переходу на IP-протоколы остается не технологическая сложность, а инерция мышления. Выбор часто делают на основе устаревших представлений о надежности FC и рисках использования IP-сетей, игнорируя радикальные изменения последних лет. Однако экономические факторы и необходимость технологического суверенитета неизбежно будут подталкивать рынок к более широкому внедрению IP-решений в системах хранения данных.



Полный текст статьи
читайте на
www.iksmedia.ru

ABSolite: бесперебойное электропитание от надежного поставщика

**Выбор современных
надежных решений
от проверенного партнера,
обеспечивающего высокий
уровень сервиса на
каждом этапе работы, –
залог того, что без энергии
ЦОД не останется.**



Рост количества данных центров и их мощностей, подхлестываемый цифровизацией и развитием ИИ-систем, требует активного внедрения новых технологий и решений – более эффективных, надежных и масштабируемых. ЦОДы, промышленные предприятия, объекты КИИ заинтересованы в партнерстве с надежными поставщиками, которые понимают нужды заказчиков, соблюдают SLA и предлагают современные эффективные решения, удовлетворяющие их запросам.

«Абсолютные Решения», компания с четвертьвековой историей, развивает собственный бренд ABSolite и соответствует всем этим требованиям. ABSolite занимается проектированием и поставкой систем бесперебойного и гарантированного электропитания для высокотехнологичных объектов, в том числе для данных центров. Компания накопила огромный опыт работы с предприятиями разного размера и сферы деятельности. Она не просто устанавливает оборудование под ключ, но охватывает весь его жизненный цикл, от разработки проекта, профессиональной установки и наладки до последующего сопровождения. Специалисты ABSolite проводят регулярное техобслуживание и мониторинг систем, служба технической поддержки работает в режиме 24 × 7. Также ABSolite оказывает помощь в

обучении персонала службы эксплуатации заказчика, что позволяет последнему более эффективно эксплуатировать установленное оборудование.

Ассортимент решений бренда ABSolite широк. Сюда входят системы накопления энергии, дизельные электростанции, станции зарядки электрифицированного транспорта (в том числе электромобилей), источники бесперебойного питания (ИБП), аккумуляторные батареи (АКБ).

ИБП

В случае сбоя в энергосети ИБП поддерживает функционирование потребителей до тех пор, пока не включится резервный источник питания (генераторная установка) или не стабилизируется напряжение. Закономерно, что к выбору ИБП необходимо подходить очень тщательно.

Модульные онлайн-ИБП ABSolite MODA разных серий мощностью 10–1200 кВА подходят для использования в ЦОДах, серверных помещениях и на предприятиях связи. Данные ИБП совместимы с литиевыми батареями.

Трансформаторные ИБП двойного преобразования ABSolite IQ33 и DL33 мощностью 10–600 кВА чаще применяются в промышленности и на предприятиях ТЭК. Эти ИБП имеют повышенную защиту от внешних факторов промышленной среды, снабжены вентиляторами с резервированием N+1, допускают подключение нескольких устройств



в параллель, что позволяет подбирать мощность системы ИБП под конкретные нужды на объектах.

Бестрансформаторные ИБП двойного преобразования ABSolite FLEX33 мощностью 10–200 кВА позволяют варьировать количество VRLA-батарей в последовательной цепи, что дает возможность подключения батарей, уже имеющихся на объекте.

АКБ

«Сердце» ИБП – это аккумуляторные батареи. ABSolite предлагает широкий ассортимент профессиональных АКБ, выполненных по разным технологиям и предназначенных для разных приложений и отраслей. В ассортименте компании есть батареи для ИБП, телекоммуникационных станций, «зеленой» энергетики, автономных систем энергоснабжения и др. Отличительные черты АКБ ABSolite – хорошие разрядные характеристики и повышенная энергоотдача. Обращают на себя внимание свинцовые батареи с увеличенным сроком службы. Так, серия ABSolite S/NF (65–200 А·ч) на базе аддитивной свинцово-углеродной технологии имеет срок службы до 20 лет. Есть и традиционные свинцово-кислотные аккумуляторы, которые за счет применения новейших технологий и использования специальных сплавов прослужат до 15 лет. Можно отметить такие линейки, как ABSolite S/HR (320–800 Вт/элемент) и ABSolite SFT/HR-700RW (700 Вт/элемент).

ABSolite Smart Li

Хотя свинцово-кислотные АКБ остаются наиболее распространенными в ЦОДах, в последние годы растет популярность решений на базе лития. Они долговечнее, компактнее, надежнее. Несмотря на более высокую стоимость, литиевые АКБ служат вдвое дольше обычных свинцово-кислотных, так что на практике разница в цене себя оправдывает. Если же оценивать полную стоимость владения, то здесь преимущество однозначно на стороне лития.

В основе системы ABSolite Smart Li – литий-железо-фосфатные (LiFePO₄, LFP) аккумуляторы. Они безопасны в ис-

пользовании, обладают прекрасными массогабаритными характеристиками, способны работать при высоких (до 40°C) температурах без потери эффективности, выдерживают от 1,5 до 2,5 тыс. циклов заряда – разряда.

При установке на объекте требуемое количество АКБ собирается в отдельные кластеры. В одном фрейме можно разместить до 10 батарейных модулей емкостью 40–200 А·ч. Система объединения и параллельное управление несколькими кластерами обеспечивают высокую степень автоматизации, а возможность параллельного подключения нескольких шкафов АКБ позволяет гибко масштабировать систему. При необходимости кластеры можно отключать.

Для управления системой ABSolite Smart Li предусмотрена функция централизованного мониторинга. Она позволяет управлять всеми кластерами АКБ, оперативно реагировать на любые изменения в работе системы, проводить предварительную диагностику, выявлять и устранять неисправности.

Все данные о работе системы ABSolite Smart Li выводятся на ЖК-дисплей с сенсорным управлением, он же используется для настройки параметров АКБ. По дополнительному информационному каналу между BMS (системой контроля батарей ABSolite Smart Li) и контроллером ИБП ABSolite обобщенная информация о состоянии АКБ выводится на дисплей ИБП. Немаловажно, что ABSolite Smart Li обеспечивают высокую энергоэффективность и крайне малые потери энергии, что способствует снижению эксплуатационных расходов и уменьшению углеродного следа.

Ознакомиться с продуктами ABSolite можно в шоуруме, где проводится демонстрация и тестирование оборудования.

ab-solution.ru

7 (495) 103-14-12

info@ab-solution.ru



Гонка суперкомпьютеров: обойти на повороте

Суперкомпьютеры переходят в эксафлопсную эру. Россия отстает, но при достаточном финансировании сможет преодолеть эксафлопсный рубеж, в том числе за счет использования альтернативных подходов.

Николай Носов

Борьба лидеров

В последнем рейтинге Top500 самым мощным суперкомпьютером стал американский El Capitan (рис. 1), который показал на тесте Linpack (HPL) производительность, равную 1 742 петафлопс (1,742 эксафлопс). Система построена на базе процессоров AMD четвертого поколения EPYC 24C 1,8 ГГц и ускорителей AMD Instinct MI300A с использованием инженерной инфраструктуры от Hewlett Packard Enterprise (Slingshot-11, HPE Cray EX). В решении задействован интерконнект с рекордными характеристиками, созданный на основе разработок компании Cray, которую несколько лет назад приобрела HPE.

El Capitan – третья система, достигшая эксафлопсной скорости вычислений, после Frontier и Aurora. Работающая в облаке Microsoft Azure в США Eagle занимает четвертое место и остается в рейтинге Top500 самой высокопроизводительной облачной системой. Ее результат HPL составляет 561,2 Пфлопс.

Еще один новый суперкомпьютер в Top500 – HPC6 – на пятом месте. Эта машина установлена в итальянском центре Eni S.p.A в Феррера-Эрбоньоне и имеет ту же архитектуру, что и система Frontier, находящаяся на второй строчке рейтинга. HPC6 – самый быстрый суперкомпьютер в Европе с HPL, равным 477,90 Пфлопс.

Отставание или задержка в развитии?

Отставание России в гонке суперкомпьютеров увеличивается. Список Top500 покинул суперкомпьютер MTS GROM компании МТС, а новых не появилось. В результате в списке осталось только шесть установленных в России систем, лучшая из которых, «Червоненки» компании «Яндекс», занимает в мировом рейтинге 60-е место и в 93,4 раза уступает в производительности лидеру. «Яндексу» также принадлежат суперкомпьютеры «Галушкин» (№ 86 в Top500)

Рис. 1. Лидер гонки суперкомпьютер EL Capitan



Источник: techpowerup.com

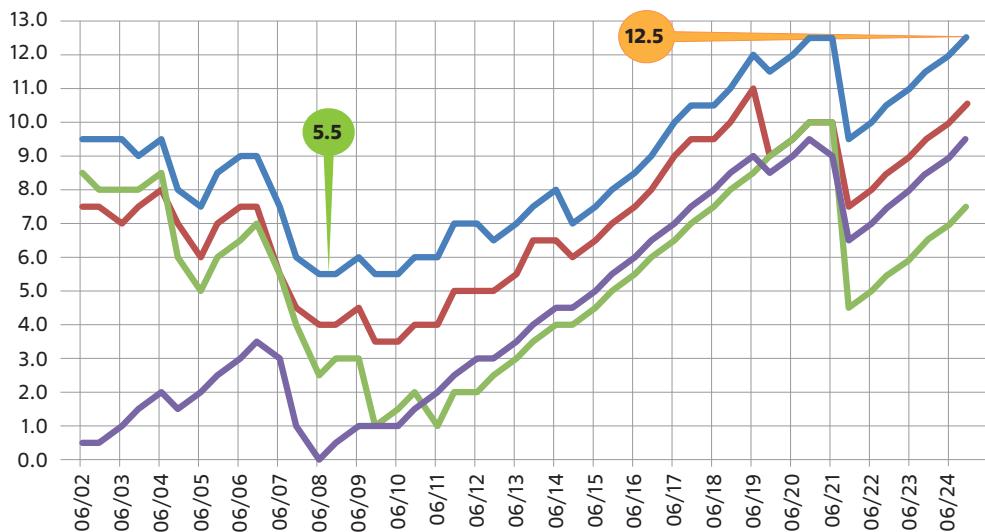


Рис. 2. Отставание России в годах по сумме Rmax от США (US), Евросоюза (EU), Китая (CN) и Японии (JP), ноябрь 2024 г.

US
EU
JP
CN

Источник:
ИПС им. А.К. Айламазяна РАН

и «Ляпунов» (№ 99). Два суперкомпьютера установлены в Сбербанке: Christofari Neo (№ 104) и Christofari (№ 172). Единственный российский некоммерческий суперкомпьютер рейтинга – «Ломоносов-2» (№ 453) принадлежит МГУ им. М.В. Ломоносова и изготовлен российской компанией «Т-Платформы». «Ломоносов-2» входит в Top500 более 10 лет – уникальное для таких систем «долгожительство». В итоге отставание России от лидирующих США по совокупной вычислительной мощности суперкомпьютеров из Top500 (Rmax) увеличилось и достигло 12,5 лет (рис. 2).

Улучшить картину могла бы новая мощная российская вычислительная система «МГУ-270» (рис. 3), о

Развитие традиционных электронных вычислителей замедляется, энергопотребление увеличивается, становятся видны физические пределы повышения производительности процессоров

которой рассказывалось на Национальном суперкомпьютерном форуме, прошедшем в ноябре 2024 г. в Переславле-Залесском. По оценкам экспертов, она вошла бы в рейтинг Top500, если бы туда были поданы соответствующая заявка и протоколы измерения Linpack-производитель-

ности. Но создатели и эксплуатанты системы такую заявку не подали, поэтому «МГУ-270» официально в число суперкомпьютеров не входит.

Принципиальную схему суперкомпьютера (рис. 4) можно представить как набор вычислительных узлов, в общем случае включающих центральный процессор (CPU), оперативную память (RAM), жесткие диски (HDD) и ускорители (Acc), в качестве которых в настоящее время чаще всего используются графические ускорители (GPU). Узлы, которых в суперкомпьютерах десятки тысяч, объединены интерконнектом (Interconnect) – системной сетью, ключевой инфра-

Рис. 3. Суперкомпьютер «МГУ-270»



Источник: МГУ им. М.В. Ломоносова

[инфраструктура]

структурой для проведения сверхбыстрых вычислений. Интерконнект позволяет узлам работать над одной задачей как слаженный оркестр. Кроме этого, есть вспомогательная сеть (TCP/IP) для доступа к узлам и обмена с ними данными из внешних сетей и сервисная – для мониторинга и контроля. Иногда добавляется сеть синхронизации для организации параллельного программирования.

Помимо вычислителя в суперкомпьютере нужно организовать хранилище данных, подвести электропитание необходимой мощности, реализовать систему охлаждения, разработать программное обеспечение и обеспечить безопасность.

Несколько лет назад Департамент энергетики США выделил 10 направлений, разработки в которых необходимы для построения суперкомпьютера эксафлопсной производительности. В их числе – решение проблем энергоэффективности, интерконнекта, увеличения емкости и пропускной способности памяти, управления данными и создание сред программирования с массовым параллелизмом. В нашей стране уже есть результаты мирового уровня в технологиях охлаждения, интерконнекта и системах программирования.

При наличии соответствующей государственной поддержки Россия может решить

оставшиеся проблемы и составить реальную конкуренцию лидерам. Особенно, если будет действовать не в одиночку, а в кооперации со странами ЕАЭС. Концепция создания межгосударственной программы «Евразийская информационно-вычислительная инфраструктура» утверждена еще в 2022 г. Но на этапе перехода от концепции к программе работы забуксовали из-за отсутствия финансирования, и будущее проекта выглядит туманным.

Фотонный цифровой процессор

Развитие традиционных электронных вычислителей замедляется, энергопотребление увеличивается, становятся видны физические пределы повышения производительности процессоров. Все это заставляет искать альтернативные подходы к архитектуре суперкомпьютера.

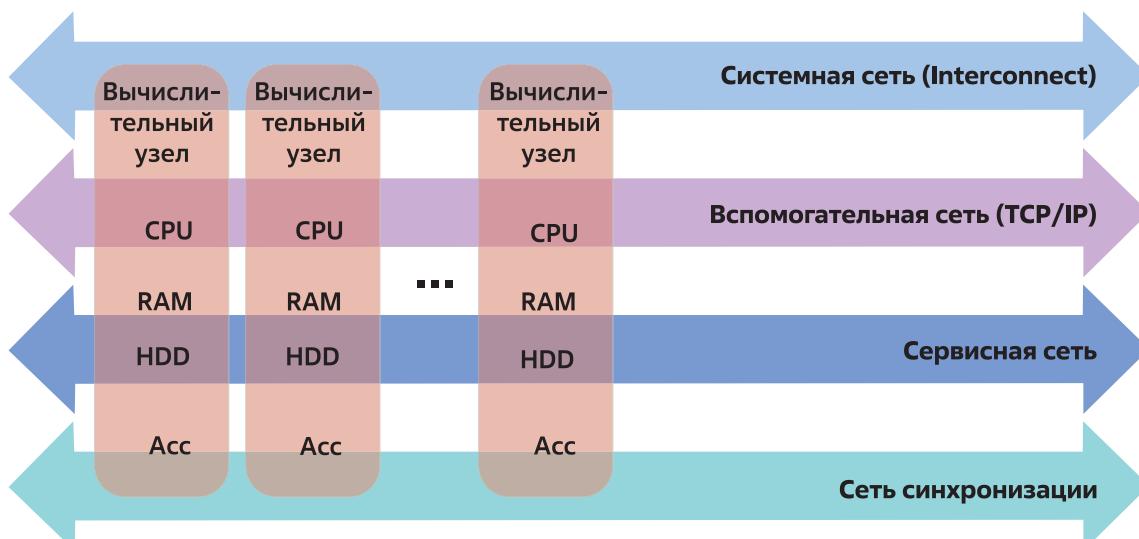
Фотонный процессор в 10 тыс. раз быстрее электронного, он может выполнять несколько задач одновременно, разделяя по длине волны свет, заменяющий электрический сигнал

Перспективным выглядит направление фотонных цифровых процессоров. У них та же двоичная система счисления с нулями и единицами, схожая система команд, но вместо электрического сигнала используется луч. Вычислительное задание преобразуется в оптическую программу, выполняя которую лазер посылает когерентные лучи в устройство ввода-вывода и дальше в процессорные блоки. Когерентность позволяет лучам взаимодействовать в оптических элементах.

В области фотонных цифровых процессоров у России, судя по докладу главного научного сотрудника РФЯЦ-ВНИИЭФ (г. Саров) доктора физ-мат. наук Сергея Степаненко, есть серьезный задел. По его словам, на фотонных технологиях можно создать арифметико-логическое устройство и память, причем с такими характеристиками, что система эксафлопсной производительности будет помещаться в поллитровой кружке, а отводимое тепло составит около сотни ватт. «Есть планы, подтвержденные результаты, патенты. Этот путь проходим», – уверен он.

«У фотонного вычислителя есть еще одно фантастическое преимущество – в отличие от CPU, который в каждый момент времени решает одну задачу, фотонный процессор может выполнять несколько задач одно-

Рис. 4. Принципиальная схема вычислителя суперкомпьютера



временно, разделяя заменяющий электрический сигнал свет по длине волны, или, в терминах телекома, используя лямбда-свитчинг. Мало того, что фотонный процессор в 10 тыс. раз быстрее электронного при том же энергопотреблении, его быстродействие можно умножить на параллельность, невозможную в электронном мире. Институт программных систем им. А.К. Айламазяна мог бы взять на себя работы по созданию программного обеспечения для такой машины», – добавил председатель оргкомитета НСКФ член-корреспондент РАН Сергей Абрамов.

Квантовый компьютер

Другое перспективное направление, квантовые компьютеры – вычислительная архитектура, построенная на принципах квантовой механики. В отличие от классических компьютеров, которые используют биты (0 и 1), квантовые компьютеры задействуют кубиты. Кубиты могут находиться в состоянии 0, 1 или в суперпозиции этих состояний, что позволяет им выполнять множество вычислений одновременно. Для создания сложных вычислительных процессов используется свойство запутанности кубитов.

Пока до конца непонятно, удастся ли создать универсальный квантовый компьютер, но вероятность создания эффективных специализированных вычислителей достаточно велика. Если говорить о суперкомпьютерах, то, скорее всего, квантовые вычислители будут выступать в качестве внешнего ускорителя для отдельных задач. Во всяком случае к этому готовятся в Юлихском су-

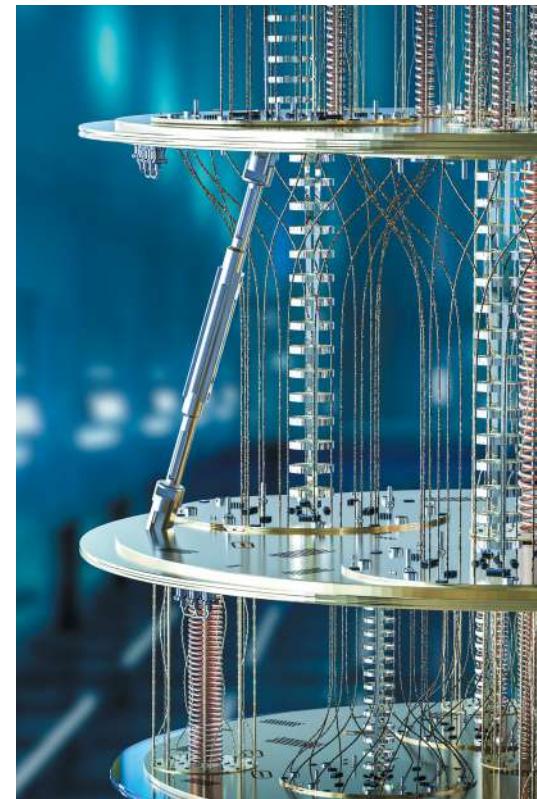
перкомпьютерном центре в Германии, где собираются использовать квантовое решение компании IQM Quantum Computers в качестве дополнения к суперкомпьютеру Jupiter, который должен стать первой европейской машиной эксафлопсного класса. Два модуля комплекса уже смонтированы.

Квантовые компьютеры
задействуют кубиты, которые
могут находиться в состоянии 0, 1
или в суперпозиции этих состоя-
ний, что позволяет
им выполнять множество
вычислений одновременно

Биологические вычислители

Еще одна альтернатива традиционным электронным компьютерам – биологические вычислители, использующие биологические молекулы (белки и нуклеиновые кислоты). Например, белки могут связываться и менять свою структуру в ответ на определенные изменения условий, что позволяет им выполнять логические операции. Выигрыш в вычислениях на молекулах основывается на огромном параллелизме.

Биологические вычислители позволяют моделировать сложные биологические процессы, что делает их полезными в таких областях, как биоинформатика и вычислительная биология. Работы ведутся давно, но первые серьезные результаты по-



лучены только в 2024 г. В январе в США создали гибридный процессор из электронных компонентов и мозгового органоида, выращенного из стволовых клеток человека. Система, названная Brainoware, способна распознавать речь и решать нелинейные уравнения.

Еще в 2014 г. в США стартовала программа по изучению человеческого мозга BRAIN с общим бюджетом в \$4,5 млрд на 20 лет. В Евросоюзе на десятилетний «Проект человеческого мозга» выделен 1 млрд евро. С десятилетним планом финансирования в размере \$1,66 млрд реализуется проект «Мозг Китая» у нашего восточного соседа.

Лидирующий суперкомпьютер занимает целое здание и потребляет 30 МВт. Мозг человека имеет объем в среднем 1,2–1,6 л и потребляет на порядки меньше. При этом способен работать до 90 лет, а бывает, и дольше. Разработчикам суперкомпьютеров есть к чему стремиться. Путей повышения производительности и энергоэффективности много. Но для исследований нужно выделять большие деньги, а это тоже очень серьезная проблема. **ИКС**



Натриевые АКБ: на старт, внимание, марш!

Рост цен на литий вновь привлек внимание разработчиков и производителей к аккумуляторным батареям на основе натрия. ИБП с натриевыми АКБ теперь есть и в России – недавно они появились в ассортименте компании Irrop. Подробностями делится директор центра компетенций Irrop Григорий Карулин.

– В ЦОДах преобладают свинцово-кислотные аккумуляторы, но доля объектов, на которых используют литиевые АКБ, неуклонно растет. Что сейчас происходит на рынке АКБ?

– Если коротко, то литий дорожает. В 2021–2023 гг. произошел резкий скачок стоимости, а поскольку разведанные запасы этого металла невелики, прогнозируется дальнейшее подорожание. Собственно, именно постоянный рост лития в цене заставил вспомнить о натрии.

Дело в том, что технологии создания литий-ионных и натрий-ионных аккумуляторных батарей возникли почти одновременно – в 1976 г. Но в то время большее развитие получил литий, так как батареи на его основе имели большую емкость.

В 2010 г. разработка АКБ на основе натрия была возобновлена, а с 2016 г. в силу геополитических и экономических причин технология стала развиваться еще активнее.

Ключевые достижения в этой области были получены в последние два года. Но отмечу, что технологии производства натриевых и литиевых батарей схожи. Именно поэтому весь путь от лаборатории до коммерческого ис-

пользования натриевые АКБ прошли так быстро.

– В чем преимущества натриевых АКБ?

– Во-первых, в отличие от лития, натрия очень много. То есть дефицит сырья нам не грозит. Кроме того, пока литиевые АКБ будут дорожать, натриевые будут становиться все доступнее.

Во-вторых, с ростом производства стоимость натриевых АКБ будет постепенно снижаться, по прогнозам, они даже могут стать дешевле свинцово-кислотных батарей. При этом их характеристики приближены к характеристикам литиевых, а порой превосходят их.

Для наглядности сравним основные параметры.

Номинальное напряжение ячейки натриевой АКБ составляет 2,8–3,5 В. Это серединное положение между свинцовой (2 В) и литиевой (3–4,5 В).

По жизненному циклу натриевые АКБ значительно лучше свинцовых и несколько хуже литиевых (свыше 3000 циклов заряда-разряда у лития, свыше 2000 – у натрия и всего 300–500 циклов у свинца).



Теперь о тех параметрах, где натрий рекордсмен. Начнем с глубины разряда. У натриевых батарей этот показатель 100%! То есть натриевую батарею можно разрядить полностью, до нуля, и после зарядки она продолжит работу без потери характеристик, в то время как у лития этот показатель – 80–100% (на практике – не более 90%), а у свинца – 50%.

Кроме того, натриевые АКБ можно и заряжать, и разряжать при низких (около –20°C) температурах. Напомню, что литиевые АКБ в такой ситуации можно только разрядить, а вот заряжать уже придется в тепле. Что касается свинца, то для него при низких температурах невозможны ни разрядка, ни зарядка.

Натриевая батарея – абсолютный лидер по скорости зарядки: она заряжается на величину, более чем в пять раз превышающую ее емкость, в час (5С). Для лития этот показатель равен 1С, для свинца – 0,15 С. Разряд высоким током (т.е. энергию, которую можно взять от батареи одномоментно) у натрия составляет 15С, т.е. это 15-кратная емкость батареи.

Для ЦОДов скорость заряда и разряда высоким током, а также допустимая температура работы, возможно, не столь важны. Но надо помнить,

что двигатель рынка АКБ – это не дата-центры, а электротранспорт. А для этой области перечисленные характеристики весьма существенны. Кстати, уже в прошлом году китайская компания BYD выпустила две машины на базе натриевых батарей.

– Ключевой недостаток литиевых АКБ, из-за которого многие остались и остегаются переходить на эти решения, – опасность возгорания. Как обстоят дела с безопасностью у батарей на основе натрия?

– С точки зрения безопасности эксплуатации натриевые батареи однозначно выигрывают у литиевых. Они не возгораются. Более того, в натриевых батареях безопасность обеспечивается на уровне ячейки.

Каждая ячейка в натриевой АКБ снабжена специальным механическим предохранителем, который сработает в случае подачи на него слишком большого напряжения и выведет батарею из строя. Вернуть его в исходное состояние не получится, но ячейку со сработавшим предохранителем можно вынуть из массива и заменить на рабочую.

Если же рассматривать вопрос с точки зрения безопасности окружающей среды, то здесь натрий также оптимален. На базе натрия создаются действительно наиболее «зеленые» на данный момент решения среди АКБ.

– Ранее Ippon сообщала о том, что тестирует натриевые батареи. Поделитесь, пожалуйста, результатами, которые были получены.

– Да, мы протестировали АКБ на основе натрия. Все перечисленные преимущества в ходе испытаний были подтверждены. Например, мы проверили, как будет заряжаться батарея, будучи предварительно полностью разряженной. За полчаса с нуля она зарядилась до 90%. Натриевые АКБ работают в широком диапазоне температур, при тестировании мы понижали температуру до -40°C .

Отмечу еще один существенный плюс: протестированные ИБП на основе натриевых батарей не только быстро заряжаются и выдерживают много-кратные циклы заряда-разряда, но и в течение долгого времени (больше года) могут не использоваться без потери рабочих качеств. Их не нужно регулярно перезаряжать, как того требуют свинцово-кислотные АКБ.

– Есть ли уже в ассортименте Ippon ИБП с натриевыми батареями? Планируете ли вы поставлять ИБП и натриевые АКБ для ЦОДов?

– Да, мы уже начали поставки однофазных ИБП с натриевыми батареями. У нас представлено несколько типов таких устройств. Это ИБП в корпусе башенного типа («тауэр») и для установки в стойку 19" (RT) мощностью от 1 до 10 кВА.



– Будете ли вы осуществлять сервисное обслуживание натриевых АКБ?

– Да, Ippon по соглашению с заказчиками полностью берет на себя обслуживание натриевых батарей.

– Замена аккумуляторных батарей одного типа на другой в ИБП не всегда возможна. Как решается эта задача в случае с переходом на натриевые АКБ?

– Никаких препятствий для замены свинцово-кислотного аккумулятора на натриевый нет. Достаточно просто заменить в ИБП батареи одного типа

на другой. Здесь не требуется ни специальных решений, ни специального оборудования. И это, конечно, огромный плюс для тех, кто хотел бы перейти на новые АКБ, но по тем или иным соображениям не готов менять источник питания.

Единственное ограничение, которое может возникнуть, связано с зарядником ИБП. Если он не поддерживает скорость заряда, присущую натриевым АКБ, то заряжаться батареи будут не так быстро, как это в них заложено. Впрочем, по сравнению со свинцовыми разница все равно будет огромна.

Что касается ИБП, использующих АКБ на основе лития, то здесь ситуация иная. Из-за требований безопасности каждая литиевая батарея большой емкости в обязательном порядке снабжается своей системой безопасности, которая на базовом уровне сопрягается с ИБП. Она становится

неотъемлемой частью ИБП, своего рода его «мозгами». Натриевые батареи в таких системах не нуждаются, потому и заменить литий на натрий не выйдет – система просто не будет «понимать» новые АКБ.

– Насколько реалистичны прогнозы о смене фаворита на рынке АКБ с лития на натрий?

– Учитывая такие факторы, как доступность элемента, близкие к литию, а порой и превосходящие характеристики натриевых батарей, потенциально низкую стоимость, можно предположить, что смена фаворита неизбежна. Полагаю, что речь идет о сроке примерно в пять лет.

Еще раз подчеркну, что ключевым рынком для АКБ являются не ЦОДы, не энергоемкие отрасли, а электротранспорт. Так что и следить за тенденциями нужно на его примере.

Пожарная безопасность ЦОДа: не автоматикой единой

Екатерина Шлык

Пожарная безопасность дата-центра должна опираться не только на современные технологические решения, но и на высокую культуру эксплуатации и строго регламентированную работу персонала. Словом, требуется комплексный подход.



За 30 лет (с 1994 по 2024 гг.) в дата-центрах зафиксирован 8 701 инцидент, причем в 12 случаях корневой причиной инцидента был указан огонь, но только в двух случаях возгорание действительно произошло, в остальных срабатывание системы раннего обнаружения пожара оказалось ложным. Такова статистика Uptime Institute, которую в ходе дискуссии «ЦОДы: тушить или не тушить. Мировой опыт и российская практика» на форуме «ЦОД-2024» привел Алексей Солодовникова, управляющий директор Uptime Institute в России и СНГ. Эти данные были получены от крупнейших операторов и владельцев ЦОДов – без преувеличения цвета глобального рынка центров обработки данных.

Может быть, дела обстоят иначе, если рассматривать картину в целом, включая «середнячков» рынка?

По данным 451 Research, в 2020–2024 гг. в мире насчитывалось от 6,5 тыс. до 7,7 тыс. дата-центров, но зафиксировано лишь 14 крупных пожаров или ложных срабатываний противопожарной системы, повлекших за собой катастрофические последствия (например, такие, как выход залитого оборудования из строя).

Как видно, относительное количество инцидентов, так или иначе связанных с пожаром, и здесь очень мало. Если взять период в пять лет, то вспоминаются единичные случаи крупных пожаров в дата-центрах. В глобальном масштабе самым нашумевшим стал пожар в ЦОДе OVHcloud в 2021 г., в российском – в дата-центре DataLine в 2019 г.

Если пересчитать количество пожарных инцидентов на количество часов работы ЦОДов и ориентироваться на статистику МЧС, то, по словам А. Солодовникова, российские дата-центры находятся примерно на уровне детских садов и оздоровительных лагерей, где уровень подобных инцидентов крайне низок.

Наконец, согласно исследованию Uptime Institute 2017 Data Center Survey (исследование проводилось однократно, поэтому увидеть ситуацию в динамике не представляется возможным), только 11% опрошенных операторов дата-центров сталкивались с пожарами в ЦОДах, в то время как 89% респондентов такого опыта не имеют.

Впрочем, несмотря на то что частота возникновения пожаров в ЦОДах сравнительно мала, риски в случае его возникновения слишком высоки, а борьба с последствиями обходится очень дорого. Поэтому вопрос не в том, надо ли тушить, а в том, как вместе с водой не выплеснуть ребенка: как в попытках предотвратить возгорание не нанести оборудованию и помещениям ущерб, сопоставимый с пожаром.

Когда тушить?

Ни у поставщиков противопожарных решений, ни у операторов ЦОДов

не вызывает сомнений необходимость использовать автоматическую систему раннего обнаружения возгорания (например, аспирационную систему), которая должна подать сигнал уже при первых признаках задымления. А вот относительно того, как действовать дальше, мнения расходятся.

Казалось бы, ответ лежит на поверхности – на сигнал нужна незамедлительная реакция, которую может обеспечить система автоматического пожаротушения. Но на практике все несколько сложнее.

Во-первых, серьезная проблема системы раннего обнаружения возгорания – ложные срабатывания. Она может детектировать не только опасный дым от готового воспламениться оборудования, но и дым от источника, не относящегося к дата-центру, скажем, от костра за пределами его территории. Например, в сети дата-центров 3data, по словам ее технического директора Максима Церуleva, за все время работы 15 ЦОДов было семь случаев срабатывания системы автоматического пожаротушения и выхода газа, но только два из них произошли по причине реального задымления. Между тем каждый раз после выхода газа систему надо заправлять заново, а это довольно дорогая процедура.

Кроме того, потенциально опасный инцидент, даже детектированный в самом дата-центре, не всегда повлечет за собой возгорание. Поэтому «тушить любой ценой» нерационально: ущерб от применения автоматического пожаротушения может быть в разы больше, чем от выхода из строя какого-либо оборудования по причине перегрева. На другой чаше весов – огромные риски развития пожара, и пропустить инцидент опасно.

Общее мнение экспертов отрасли таково: в дата-центре непременно должны быть и система раннего обнаружения, и система автоматического пожаротушения, но работа автоматики всегда должна верифицироваться людьми. Ответственные сотрудники, приняв сигнал от системы раннего

Крупные пожары в ЦОДах

2019 г., июнь. Дата-центр DataLine на Боровой (Москва, Россия). Возгорание началось под металлической крышей здания ЦОДа. Вскоре начали взрываться фреонопроводы систем холодаоснабжения. Полностью вышли из строя пять кондиционеров, у части кондиционеров сгорели кабели питания внешних блоков. Из 16 машзалов ЦОДа пострадал один. Возникли проблемы с рядом служб и сервисов, сильно пострадали некоторые офисы. Компания выплатила клиентам штрафы за все не работавшие сервисы и простоя согласно SLA, предоставила место для резервирования и помогла восстановиться.

2021 г., март. Дата-центр OVHcloud, здание SBG-2 (Страсбург, Франция). ЦОД предоставлял услуги аренды выделенных серверов и облачные сервисы. В результате инцидента частично или полностью прекратили работу веб-ресурсы по всей Европе (по имеющимся сведениям, пострадало свыше 3,5 млн веб-ресурсов). Пожаром были уничтожены 15 тыс. серверов. Больше всего пострадали данные пользователей симулятора выживания Rust – пожар уничтожил 25 серверов онлайн-игры, информация безвозвратно потеряна.



Пожар в OVHcloud

Источник: DNA.FR/Jean-Christophe Dorn

обнаружения, должны сами оценить ситуацию и решить, по какому сценарию необходимо действовать.

Система раннего обнаружения пожара, полагает заместитель директора по управлению эксплуатацией ГК Key Point Константин Нагорный,

предназначена в первую очередь для информирования людей. А регламент действий в случае инцидента должен определять главный инженер или технический директор, это их зона ответственности. Ведь при ложном срабатывании автоматической системы газового пожаротушения оператор

Система раннего обнаружения пожара

Источник: ГК «Пожтехника»

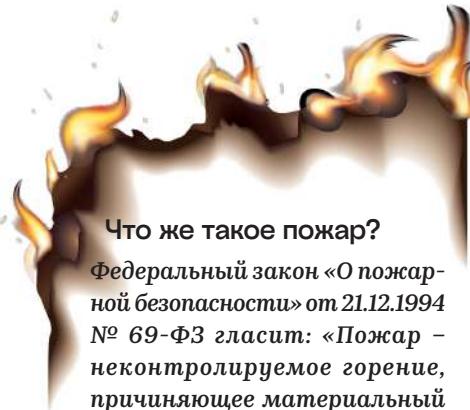
ЦОДа понесет издержки только на повторную заправку системы газом, но если на объекте установлена система тушения водой, то с оборудованием можно попрощаться – по крайней мере, на значительное время, если не навсегда.

Связку «автоматика – человек» используют на своих площадках DataSpace. Как рассказал технический директор компании Николай Шеметов, оператор ЦОДа, оказывая услуги размещения клиентского оборудования, порой сталкивается с тем, что оборудование клиента слишком старое или изношенное. Поэтому случаи перегрева и задымления возможны. Но, оценивая корректность срабатывания системы сверхраннего обнаружения и тяжесть случаев, технические специалисты всегда сверяются с данными температурных датчиков, с показателями нагрузки сети (если проблема в оборудовании, то будет скачок напряжения).

Аналогичного подхода придерживаются и в 3data. Если позволяет время и ситуация не критическая, то, как считает М. Церулов, имеет смысл тщательно оценить происходящее – с помощью систем видеонаблюдения, показателей датчиков и графиков электропитания стоек. Сотрудникам технической службы стоит пройти по проблемному участку с тепловизором. И уже в зависимости от полученных данных нужно предпринимать те или иные действия – по каждой из экстренных ситуаций в 3data есть четко расписанные инструкции для персонала. Есть она и на тот случай, когда видно открытое пламя – непременно тушить автоматически, люди к огню приближаться не должны. В такой ситуации использование автоматического пожаротушения более чем оправдано: «Если оборудование



горит с пламенем, то когда же его тушить, если не сейчас?», – уверен М. Церулов.



Что же такое пожар?

Федеральный закон «О пожарной безопасности» от 21.12.1994 № 69-ФЗ гласит: «Пожар – неконтролируемое горение, причиняющее материальный ущерб, вред жизни и здоровью граждан, интересам общества и государства».

Сходное определение пожара дает МЧС России: «Пожар – неконтролируемый процесс горения, сопровождающийся уничтожением ценностей и создающий опасность для жизни и здоровья людей, сельскохозяйственных животных, растений и окружающей среды».

Очевидно, что на первом месте должна стоять безопасность людей. Поэтому регламенты для технических служб, как указывает Сергей Манаев, заместитель генерального директора ГК «Инновационные системы пожаробезопасности», должны однозначно предписывать, что в случае видимого огня (например, он заметен на кадрах, переданных

видеокамерой из проблемного зала) необходим запуск автоматической противопожарной системы. А Михаил Кочетков, генеральный директор «Холдинг ОСК групп», полагает, что даже если открытого огня не видно, то ходить и проверять задымления технические специалисты на всякий случай должны с огнетушителями.

Однако аварийное пожаротушение – это крайняя мера, считает Петр Ронжин, заместитель руководителя дивизиона эксплуатации data-центров «Яндекса». Отказ оборудования не так страшен, как отказ в представлении сервисов. Именно сервисы должны быть в приоритете, и ничто не должно мешать их предоставлять, даже если для этого придется пожертвовать теми или иными устройствами (естественно, речь не идет о критических ситуациях, когда под угрозой оказывается буквально весь объект).

Операторы коммерческих ЦОДов придерживаются в этом вопросе противоположной точки зрения, хотя и допускают, что для корпоративного data-центра подход «Яндекса» правомерен. «Если компания считает для себя возможным пожертвовать установленным в ЦОДе оборудованием, то это ее решение», – отмечает М. Церулов. Но в коммерческом ЦОДе, убежден он, оператор всегда должен исходить из интересов заказчиков и зафиксированных SLA. Например, у клиента может быть очень дорогой



Система автоматического пожаротушения в data-центре «Яндекса»

Источник: «Яндекс»

установка любой системы должна быть оправдана и экономически, и стратегически. Это ни в коем случае не должна быть система ради системы. Например, разработчики и поставщики систем пожаротушения, стараясь продать свои продукты, нередко, по словам П. Ронжина, упирают на то, что «так прописано в нормах».

Спору нет, пожаробезопасность ЦОДа должна быть обеспечена, но это вопрос не только установки той или иной системы. Здесь нужно, с одной стороны, руководствоваться пониманием реальных рисков, а с другой – видеть цель и иметь набор решений для ее достижения. Это комплексная задача, которую надо выполнять на разных уровнях. В частности, отмечает эксперт, в общей пожаробезопасности ЦОДа немалую роль играют дизайн и подбор материалов для каждого помещения. Скажем, отказ от фальшпола в пользу голого бетона, как это реализовано в data-центрах «Яндекса», сам по себе улучшает пожаробезопасность.

ЦОД включает в себя множество различных помещений и модулей, каждое из которых имеет свои риски пожаробезопасности, свои особенности работы, свою цену выхода из строя и т.д. Для каждого модуля подходят свои системы пожаротушения, полагает П. Ронжин. Поэтому не только тем, кто строит и эксплуатирует ЦОДы, но и тем, кто предлагает системы пожаротушения для объектов, надо исходить из конкретных целей, задач и возможностей.

И наконец, стоит учесть замечание К. Нагорного, который подметил, что, говоря о пожарах в ЦОДах, все фокусируются на серверных помещениях, в то время как аварийные ситуации чаще всего возникают не там. Поэтому так важна общая культура эксплуатации ЦОДа как целостного объекта. **ИКС**

«штучный» blade-сервер, который в случае повреждения в нынешних условиях будет практически не восстановим. Так что жертвовать оборудованием клиентов оператор colocation не имеет права. Лучше запустить систему газового пожаротушения, чем рисковать, полагает эксперт.

Таким образом, автоматическое пожаротушение – единственно правильное решение для современного data-центра. Малое число пожаров в ЦОДах, особенно в ЦОДах крупных мировых игроков, по мнению Натальи Хазовой, генерального директора ГК «Пожтехника», как раз служит лучшим подтверждением необходимости использования систем такого рода: во всех data-центрах первого эшелона решения для автоматического пожаротушения установлены. Однако речь не идет о немедленном включении автоматики сразу после срабатывания системы раннего обнаружения пожара, подчеркивает Н. Хазова. Временной зазор между срабатыванием систем позволяет людям вмешаться в процесс. Но если людей не оказалось рядом или они не успели среагировать, то автоматика позволит не допустить критической ситуации.

Пожаротушение – задача комплексная

Вопрос «Если тушить с помощью автоматической системы, то какую систему использовать?» не так прост

и, следовательно, ответы на него неоднозначны. По данным уже упоминавшегося исследования Uptime Institute 2017 Data Center Survey, 18% опрошенных высказались за использование в системах пожаротушения ЦОДов воды, 54% – газа, 28% – того и другого.

За годы, прошедшие с этого исследования, технологии шагнули вперед, в частности, достаточно широкое развитие получили системы тушения водяным туманом, или тонкораспыленной водой. В России такое решение используется, например, в ЦОДе IXcellerate. Так что у воды, по всей вероятности, сторонников теперь будет больше 18%. Правда, отвечая на вопрос, какую систему выбрать для обеспечения пожаробезопасности машинных залов ЦОДов, участники дискуссии на «ЦОД-2024» почти единогласно высказались за автоматические системы газового пожаротушения. Более того, как заметил К. Нагорный, никакой клиент в коммерческий ЦОД не пойдет, если в нем не будет именно такой системы. Если же речь идет о корпоративном ЦОДе, продолжает эксперт, то здесь вариантов может быть множество. Можно заливать водой, засыпать песком, можно даже совсем не тушить – это зависит от корпоративных правил и установок.

Что же касается остальных помещений data-центра, то здесь единого мнения нет. Скорее, есть понимание того, что



Envicool: слагаемые успеха

В 2024 г. Envicool, согласно выпускаемой iKS-Consulting «Карте вендоров», упрочила свое лидерство в сегменте систем кондиционирования и вентиляции для ЦОДов. О слагаемых успехах и тенденциях рынка – Владимир Шепелев, управляющий директор российского офиса компании.

– Владимир, что помогает Envicool быть успешной на российском рынке?

– Есть несколько составляющих. Начну с технологической, куда входят качество производства и эффективность R&D. В России принято считать: «Если китайское, то, скорее всего, не очень хорошее, а если хорошее – то это надо проверить». Качество нашей продукции уже многократно проверено. Оно устраивает даже самых придирчивых заказчиков.

Когда говорят о качестве оборудования, имеют в виду качество комплектующих, качество сборки. Но я хочу обратить внимание также на контроллер. У Envicool собственный контроллер, и это большое преимущество. Свой контроллер – это гибкость и управляемость, что очень ценно для непростых цдовых проектов. Мы можем оперативно адаптировать решения под специфические требования конкретных заказчиков, подстраивать систему даже в процессе пусконаладки.

Вторая составляющая – доступность. Наши сроки поставки также полностью удовлетворяют требованиям заказчиков. В этой составляющей не менее важна доступность сотрудников компании: насколько быстро

можно дозвониться, задать вопрос, получить ответ.

Не секрет, что своевременно получить ответ на запрос бывает проблемой. Зачастую приходится ждать несколько недель. Мы не можем позволить себе так работать. С некоторыми партнерами и заказчиками у нас есть негласное SLA на скорость ответа: мы должны в течение суток полноценно ответить на входящий запрос, сформировать технико-коммерческое предложение. И конечно, большое значение имеет скорость реакции в вопросах сервиса и поддержки, в том числе постгарантийной.

– Какие тенденции вы бы отметили на российском рынке систем кондиционирования и вентиляции для ЦОДов в целом?

– Если в прошлом году рынок рос быстро, то в текущем, по нашей оценке, рост сохранится, но замедлится. Это напрямую связано с высокой ключевой ставкой, дорогими деньгами. Рынок, конечно, развивается, те, кто используют негосударственные деньги, продолжают активно строить. Но будет замедление.

– А если говорить о технологических тенденциях?

– Начну с простого. Продолжается рост температуры гликоля в чиллерных системах. Примерно 80–90% заказчиков соглашаются переходить на высокие температуры гликоля, например, на график 20–26°C. Это позволяет существенно экономить электроэнергию при гарантированном выполнении SLA перед заказчиками.

Кроме того, все больше заказчиков рассматривают альтернативные решения для систем охлаждения. Не классическую систему «чиллер – фанкойл», а, скажем, чиллер с вентиляционной стеной или просто вентиляционную стену на фреоне.

– Как меняется отношение заказчиков к фрикулингу?

– Заказчики начинают соглашаться с альтернативами, где присутствует слово «адиабатический». Раньше это категорически отвергалось: не понимали, как обслуживать, как сливать, считали опасным. Теперь уже не боятся. Обычно выбирают адиабатические системы с промежуточным теплообменником. Как правило, в качестве резерва дополнительно устанавливают фреоновый (DX) до-охладитель во внутреннем контуре.

Адиабатическое охлаждение рассматривают корпоративные, и

коммерческие ЦОДы. Кстати, в Китае многие коммерческие ЦОДы активно используют адиабатику. Правда, в Китае масштабы ЦОДов несколько иные: типовые объекты имеют мощность 50–100 МВт. Часто это здания в четыре–пять этажей, на каждом свои машзалы, все на адиабатике – очень красиво выглядит и эффективно работает.

Обязательно надо упомянуть фреоновый фрикулинг. На него много запросов. Это относительно недорогое и энергоэффективное решение, которое действительно работает.

Самое интересное – гибридный режим, когда насос (системы фрикулинга) и компрессор работают одновременно. Приведу пример из практики. При температуре на улице около +10°C потребление системы без фреонового фрикулинга достигает 40 кВт, а с подключением фрикулинга – 29 кВт. Разница примерно 25%, это приличная экономия.

Буквально в январе 2025 г. я был на заводе в Китае, где мы тестировали систему фреонового фрикулинга в различных режимах для мегаваттного ЦОДа одного российского заказчика. Заказчик попросил уменьшить время выхода на рабочий режим (Fast Restart), в том числе с включенным фрикулингом. И тут нам опять помог наш контроллер. Поиграв с уставками, мы смогли обеспечить выход на полноценный холод за 1,5 мин. Это важно, чтобы не допустить перегрева ИТ-оборудования.

– Хайп вокруг ИИ резко повысил интерес заказчиков к высоконагруженным стойкам. Какие запросы приходят к вам, какие технологии предлагаете?

– Соглашусь, во многом это хайп. Но заказчики проявляют интерес, мы получаем запросы на жидкостное охлаждение для стоек мощностью 25–60 кВт. Мы это просчитываем, но в достойном объеме до реализации дела пока не дошло. Речь идет о жидкостном контактном охлаждении с использованием охлаждающих пластин, накладываемых на CPU и

другие наиболее горячие элементы ИТ-оборудования.

20–25 кВт – это тот экономически и технологически обоснованный предел, до которого хорошо работает воздушное охлаждение.

Реальных внедрений систем с прямым жидкостным охлаждением в России у нас пока нет. В КНР таких проектов много, общая мощность уже работающих подобных систем достигает 3 ГВт. Подчеркну, что в китайских ЦОДах высоконагруженные стойки с жидкостным охлаждением имеют мощность 20–25, максимум 30 кВт, т.е. намного ниже тех хайповых запросов, которые поступают нам в России.

– Есть мнение, что в России проблемы с внедрением высоконагруженных систем с жидкостным охлаждением во многом обусловлены отсутствием соответствующих серверов.

– В нашем портфеле помимо всей необходимой охлаждающей инфраструктуры (блока CDU, различных гребенок, наружных блоков и т.д.) есть и охлаждающие пластины. В Китае компания работает непосредственно с производителями чипсетов и серверного оборудования, и они используют эти пластины для охлаждения своих устройств. В России мы тоже планируем сотрудничать с ведущими производителями серверов, чтобы заказчикам были доступны серверы с уже установленными охлаждающими пластинами, которые можно просто и быстро подключить к нашей охлаждающей инфраструктуре.

– Как Envicool развивает сервис, складскую программу?

– Мы продолжаем обучение персонала авторизованных сервисных центров по всей стране с акцентом на удаленные регионы. В Москве, Санкт-Петербурге, Екатеринбурге, Новосибирске все понятно. А вот чем дальше, тем нагрузка на логистику и людей становится больше. Поэтому эта работа очень важна.

Оборачиваемость склада ЗИП мала. Это говорит о высоком качестве обо-

рудования. Случай выхода из строя компрессора или вентилятора можно пересчитать по пальцам. Когда из примерно 5 тыс. вентиляторов за все время эксплуатации вышло из строя три, это хороший показатель. Это плюс. Минус в том, что обновления склада не происходит. Хранить запасные компрессоры и вентиляторы более пяти лет неправильно, поэтому скоро займемся обновлением склада ЗИП.

Есть на складах и готовые комплекты. Это главным образом рядные кондиционеры, которые часто используют в небольших проектах. Рядные решения имеют наибольшую оборачиваемость, расходятся очень хорошо. Со шкафными сложнее попасть в нужную конфигурацию. Но такие продукты тоже есть на складе. Склад помогает и в экстренных ситуациях, когда надо быстро привезти оборудование на площадку.

– Удержать лидерство зачастую сложнее, чем его завоевать. Что планируете делать для этого?

– Согласен, удержать действительно сложнее. У нас сотни заказчиков и партнеров, и к каждому нужен индивидуальный подход. Это непросто. Нужны качественные человеческие ресурсы. Мы щепетильно и тщечно подходим к выбору кадров. И тщательно выстраиваем внутри команды процессы, кто за что отвечает, чем занимается.

К сожалению, сегодня ситуация на рынке такова, что многие компании подходят к проектам поверхностно: «выиграть тендер несмотря ни на что, а там будь что будет». Нет комплексного подхода, охватывающего сервисное обслуживание, гарантийную и постгарантийную поддержку. Мы же придерживаемся именно комплексного подхода. И наряду с теми преимуществами, о которых я говорил вначале, это поможет нам сохранить лидирующие позиции на рынке.



Брачные игры павлинов, или Проблемы выбора системы виртуализации

Рынок отечественного ПО виртуализации ИТ-инфраструктуры растет двузначными темпами. Однако переход на российские решения осложняется необходимостью выбора из большого числа непроверенных продуктов.



Николай Носов



Переход необходим

Ландшафт отечественного рынка систем виртуализации кардинально изменился и даже в случае положительных геополитических сдвигов уже не станет таким, как прежде. Причем дело не только в уходе из России зарубежных вендоров и потере доверия к их продуктам. Мирового лидера, с большим отрывом опережавшего конкурентов и на российском рынке, компании VMware как самостоятельной единицы больше не существует – в мае 2022 г. ее купила Broadcom. «Мы плохо осознаем, что произошло в индустрии. Старой добрых платформы VMware vSphere, которую покупаешь и потом используешь всю жизнь, теперь нет», – констатировал на конференции IT Elements 2024 директор департамента виртуализации и контейнеризации компании «Инфосистемы Джет» Дмитрий Горохов. Компания Broadcom сфокусировалась на получении максимума прибыли от топовых заказчиков, предложив остальным модель подписки – вариант для российских пользователей малопривлекательный.

Поддержка VMware vSphere 7.0, которой пользуется большая часть рынка, прекратится 2 апреля 2025 г. Продукт больше не будет развиваться, а главное, перестанут появляться обновления, устраниющие уязвимости безопасности. «Жить на софте без обновлений – все равно что на бомбе замедленного действия, которая начинает тикать с момента прекращения поддержки», – так выразительно описал проблему директор по развитию бизнеса «Орион софт» Максим Березин.

Тем не менее российский бизнес пока не слишком торопится и продолжает использовать старые версии продуктов зарубежных вендоров, по-разному решая вопросы обнов-

ления и поддержки. Однако «процесс пошел», и одни задумываются о переходе на российские продукты сами, другие – под воздействием регулятора. Рано или поздно заменять импортные системы придется, причем владельцам значимых объектов КИИ скорее рано. «Основные потребители российских платформ виртуализации – организации с критической информационной инфраструктурой. После того как компания наработает экспертизу по эксплуатации новой платформы, эта платформа начинает использоваться не только в КИИ. А некоторые заказчики приобретают продукты на основании технических характеристик и ценовой политики, не будучи обязаны соблюдать требования регулятора», – дал комментарий нашему изданию директор по стратегическому развитию НТЦ ИТ РОСА Вячеслав Кадомский.

Одно не вызывает сомнений – перед компаниями встал нелегкий выбор системы из множества, включенных в Единый реестр российских программ для ЭВМ и баз данных (ЕРРП).

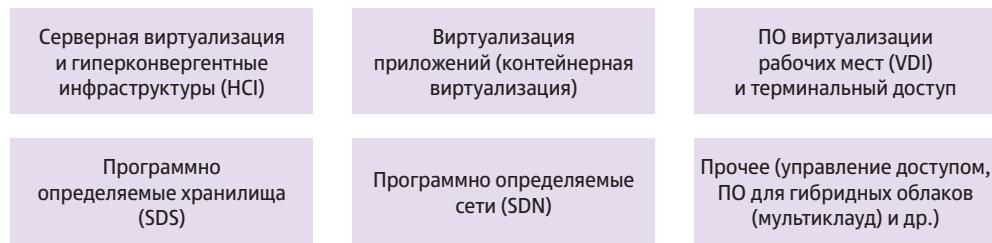
Брачные игры вендоров

«Выбор из 20–30 российских вендоров виртуализации похож на брачные игры павлинов, когда самки по хвосту выбирают самого красивого самца. Многие вендоры «распускают хвосты», делают их максимально красивыми, чтобы привлечь заказчика, иначе с ними даже не станут разговаривать», – провел аналогию независимый эксперт, экс-сотрудник VMware Андрей Коновалов.

Сравнение корректное. Видел в африканском национальном парке, как павлин, издавая дребезжащий звук, вышел на поляну, раскрыл веером хвост и начал медленно вращаться. Увидев торчащий из кустов веер, к «танцплощадке» довольно быстро

Рис. 1. Таксономия рынка ПО виртуализации ИТ-инфраструктуры

Источник: iKS-Consulting



прибежали четыре самки, оценивая сексуальную и физическую форму кандидата на спаривание.

Громко заявить о своем продукте в СМИ, а потом «распустить хвост» во время презентации – подход нормальный, основа бизнеса. А вот выбирать партнера только на основании рекламных буклотов опасно. Правильнее сформировать лонг-лист из реально работающих, имеющих внедрения российских решений, исходя из своих потребностей, составить короткий список, внеся в него системы с заявленным необходимым функционалом, и провести тщательное тестирование. По такому пути, как рассказал главный архитектор «РСХБ-Интех» Илья Калашников, пошли в Россельхозбанке.

Так же поступили в аэропорту Шереметьево. «Пришло требование регулятора: к концу года мы должны перевести объекты КИИ на отечественную виртуализацию. Выбрали 15 решений из реестра, прошлись по основному функционалу, составили шорт-лист и развернули тестовые стенды для трех систем, набравших максимальные баллы. В основном смотрели на соблюдение требований ФЗ-187 и отказоустойчивость», – по-

делился опытом импортозамещения главный эксперт по инженерным системам ЦОД аэропорта Шереметьево Александр Крылов.

Формирование лонг-листа

Прежде всего компания, исходя из бизнес-задач, должна определить архитектуру новой ИТ-инфраструктуры и типы используемых решений виртуализации (рис. 1).

Затем нужно сформировать лонг-лист, что уже является проблемой. Даже поиск решений в ЕРРП – задача непростая. А еще надо понять, действительно ли этот продукт доступен сегодня, когда компании быстро появляются и так же быстро исчезают, оставляя свои решения в реестре, и имеет ли он реальные внедрения.

В формировании лонг-листа поможет выпускаемая «ИКС-Медиа» карта российских решений виртуализации, которая ежегодно обновляется. Но в условиях турбулентного рынка даже год выглядит большим сроком. Для получения оперативной информации стоит следить за публикациями в СМИ.

Виртуализация – важнейшая часть инфраструктуры, на которой строится ИТ-ландшафт предприятия. Фунда-

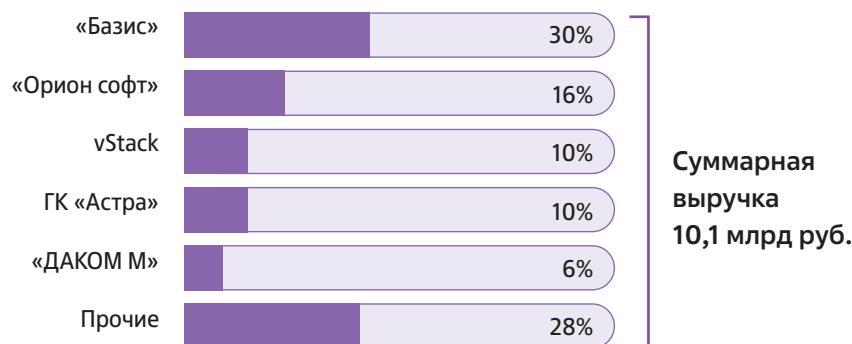
мент должен быть прочным, причем как в плане бесперебойной работы программного обеспечения, так и в плане надежности его поставщика. Надежность во многом связана с положением компании на рынке и ее размерами – чем больше компания, тем больше у нее ресурсов.

Важную роль играет и реклама. Если компания в нее вкладывается («разворачивает веером хвост»), значит, заинтересована в росте числа клиентов, своей доли на рынке и имеет для этого достаточно ресурсов. Это подтверждают и результаты анализа рынка виртуализации, проведенного iKS-Consulting (рис. 2). В лидерах – «Базис», «Орион софт», ГК «Астра» и vStack («ИТГЛОБАЛКОМ Лабс»), наиболее активные в плане рекламы в СМИ и на конференциях.

По рекламе во многом можно судить о перспективах продуктов. Если компания купила конкурента, а потом не рекламирует его решение, то, скорее всего, сделала покупку ради какой-то интересной части, например оркестратора, или перспективной команды, которая усилит основной продвигаемый продукт покупателя. Купленное решение останется в ЕРРП, его будут какое-то время поддержи-

Рис. 2. Конкурентные позиции крупнейших российских игроков рынка ПО виртуализации ИТ-инфраструктуры, доля суммарной выручки российских вендоров, 2023 г.

Источник: iKS-Consulting



вать, но выбирать это ПО для нового проекта слишком рискованно – наибольшее внимание будет уделяться основному продукту и именно на него будут пытаться перевести новых клиентов.

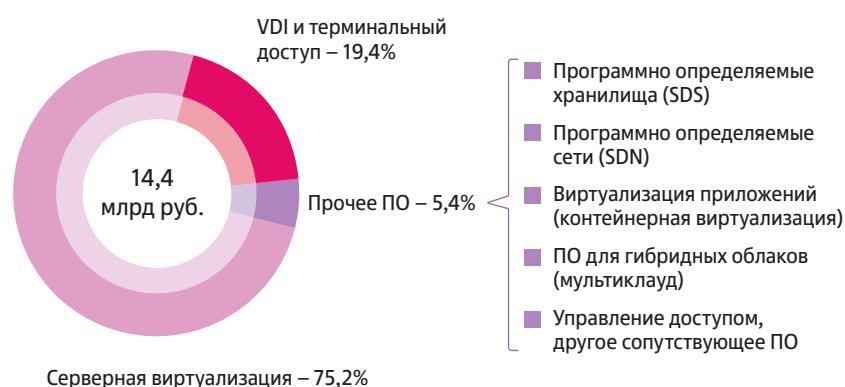
Другой показатель – наличие крупных якорных заказчиков. Если они системообразующие для государства, то вендору будут помогать поддерживать и развивать продукты. Например, надежными выглядят решения «Базиса», на которых работает цифровая платформа органов власти «Гостех», или удовлетворяющие повышенным требованиям безопасности продукты ГК «Астра», которые применяются в государственных структурах, обязанных такие требования соблюдать.

Используемые технологии

В истории с павлином в Африке самец потерпел неудачу. Придирчивые самки некоторое время наблюдали за его великолепным танцем, но из соседних кустов раздались призывающие крики соперника, и они бросились к нему в поисках более интересного кандидата. Мало привлечь к своему решению внимание заказчиков, надо доказать, что для них оно лучшее. Или хотя бы лучшее из доступных на рынке.

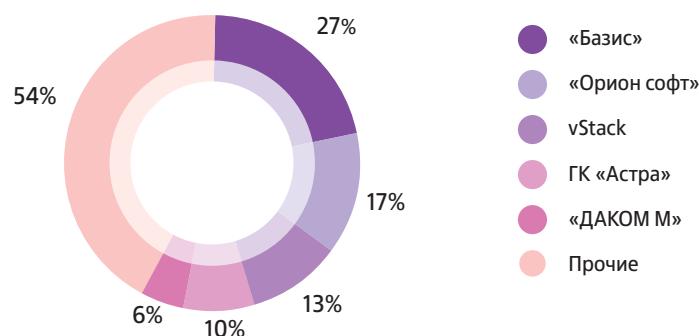
Прежде всего надо разобраться с решениями серверной виртуализации. На их долю, по оценкам iKS-Consulting, приходится 75,2% российского рынка виртуализации ИТ-инфраструктуры (рис. 3 и 4). Основные компоненты серверной виртуализации – гипервизор, обеспечивающий виртуализацию сервера (хоста), и система управления, отвечающая за оркестрацию и безопасность. Таких решений, действительно работающих и имеющих внедрения, в ЕРРП много (см. таблицу).

Крупные российские компании (Сбер, «Ростелеком», ВК) еще до событий 2022 г. стали использовать продукты open source – связку гипервизора KVM (KVM + QEMU) и облачной платформы OpenStack. Так же поступают многие зарубежные компании, не желающие зависеть в чувствительной для бизнеса сфере ИТ-инфраструктуры от проприетарного решения: к



Источник: iKS-Consulting

Рис. 3. Структура рынка отечественного ПО виртуализации ИТ-инфраструктуры, доля суммарной выручки российских вендоров, 2024 г.



Источник: iKS-Consulting

Рис. 4. Выручка российских производителей от ПО серверной виртуализации, доля объема всего рынка в денежном выражении, 2023 г.

примеру, Huawei «допилила» OpenStack для своего облака.

Хотя OpenStack будет работать и на двух хостах (серверах), основное его преимущество – работа на крупных кластерах. Недостаток – сложность развертывания и сопровождения, требующая квалифицированных программистов. Крупные компании могут позволить себе держать в штате таких специалистов, чтобы дорабатывать OpenStack под себя. Менее крупные рассчитывают на поддержку вендоров – платформа в основном используется в проектных решениях, предполагающих, что ПО модифицируется вендором в соответствии с требованиями заказчика.

Это справедливо и для других базирующихся на open source системах

управления виртуализацией (Open Nebula, oVirt, Proxmox). Из них наиболее удобна для сопровождения система oVirt, на базе которой появилось много российских продуктов. В стране мало компаний масштаба Сбера, которым требуется кластер на тысячи хостов, так что можно обойтись и без OpenStack. Недостаток oVirt в том, что сделавшая ее максимально дружественной к пользователю американская компания Red Hat ушла с российского рынка, а именно она во многом определяет направления развития системы. Однако уход Red Hat освободил нишу для использующих oVirt решений российских вендоров: zVirt от «Орион софт», Rosa Virtualization от НТЦ ИТ РОСА, HOSTVM от ИК «ХОСТ», «Ред Виртуализация» от РЕД СОФТ. При переходе на эти системы россий-

ским пользователям Red Hat даже не пришлось переучиваться.

Есть у компаний специалисты по решениям open source или нет, она все равно попадет в зависимость от вендора ПО. Да и построенные на базе open source российские продукты далеко ушли от поддерживаемых сообществом «ванильных» версий, поэтому можно сразу выбирать решения, основанные на собственных разработках вендоров. Среди лидеров этого сегмента – «Базис», vStack и «ДАКОМ М».

Стремясь выделиться среди конкурентов, компании подчеркивают технологические изюминки своих продуктов. Так, vStack делает акцент на уникальность «легкого», мини-

мально задействующего ресурсы CPU гипервизора на базе bhyve. «ДАКОМ М» – на модный искусственный интеллект: технология FreeGRID позволяет без лицензионных ограничений нескольким виртуальным машинам совместно использовать возможности аппаратного ускорения видеокарты Nvidia. ВК заявляет, что установивший их платформу заказчик получит в своем контуре с полным контролем полноценное облако с маркетплейсом и широким спектром продвинутых сервисов IaaS, PaaS и SaaS. А Selectel упирает на вертикальную интеграцию – поставку не только облака, но и подогнанной под него своей ОС и даже разработанных компаний серверов.

Российские рыночные решения серверной виртуализации

Виртуализация	Система управления	Решение	Правообладатель	Рег. номер и дата включения в ЕРРП
KVM + QEMU	OpenStack	Облачная платформа КРОК (К2 Облако)	КРОК («К2 Интеграция»)	№ 5386 от 06.05.2019
		Облачная платформа Selectel	Selectel («Селектел»)	№ 9884 от 25.03.2021
		VK Cloud (Облако Mail.ru)	ВК	№ 10379 от 21.04.2021
		«Т1 Облако» (Облачная платформа ВТБ)	ВТБ	№ 11873 от 22.10.2021
		«Рокит Клауд»	«Рокитсофт»	№ 16035 от 23.12.2022
	oVirt	Облачная платформа KeyStack	«Ключевые ИТ решения»	№ 16130 от 29.12.2022
		HOSTVM («ХОСТ»)	ИК «ХОСТ»	№ 4407 от 16.04.2018
		zVirt (z Virt)	«Орион софт»	№ 4984 от 03.12.2018
	Open Nebula	ROSA Virtualization	НТЦ ИТ РОСА	№ 5091 от 10.01.2019
		«РЕД Виртуализация»	РЕД СОФТ	№ 6929 от 01.09.2020
Собственная разработка	Proxmox	ПК СВ «Брест»	«РусБИТех-Астра», ГК «Астра»	№ 3742 от 23.07.2017
		«Горизонт-ВС»	ИЦ «Баррикады»	№ 4764 от 19.09.2018
		«Альт Виртуализация»	«Базалт СПО»	№ 6487 от 07.04.2020
		Sharkx Base (Программно-аппаратный комплекс виртуализации Sharx)	«Шаркс Датацентр»	№ 22834 от 06.06.2024
	Virtuozzo	UtiNet Glovirt	«КонсалтингПроф»	№ 12444 от 30.12.2021
		«Р-Виртуализация»	«Росплатформа» («Р-ПЛАТФОРМА»)	№ 3348 от 03.05.2017
	Собственная разработка	«Кибер Инфраструктура»	«Киберпротект»	№ 6402 от 07.04.2020
		VMmanager	«ИСПсистем», ГК «Астра»	№ 790 от 16.05.2016
		Veil	НИИ «Масштаб»	№ 4608 от 05.07.2018
		«Базис.Cloud»	«Базис»	№ 8740 от 31.12.2020
		vAIR	«Аэродиск»	№ 8802 от 31.12.2020
Xen	Xen Orchestra	SpaceVM	«ДАКОМ М»	№ 16085 от 29.12.2022
		«Ситроникс Платформа виртуализации»	«Ситроникс»	№ 16518 от 03.02.2023
bhyve	Собственная разработка	Numa vServer	«Нума Технологии»	№ 13854 от 07.06.2022
		V-Софт	БСС	№ 18712 от 22.08.2023
		vStack	vStack («ИТГЛОБАЛКОМ Лабс»)	№ 11995 от 18.11.2021

Примечание: в скобках приведены названия решений и компаний, их разработавших, под которыми они зарегистрированы в ЕРРП.

Источник: ЕРРП и данные компаний

Важное преимущество – наличие экосистемы совместимых продуктов виртуализации, включающей VDI, SDS, системы обеспечения безопасности, резервного копирования и восстановления. Разветвленные экосистемы продуктов из ЕРРП предлагают «Базис», ГК «Астра» и «Орион софт».

К виртуальной инфраструктуре нужно обеспечить удаленный доступ. Поэтому неудивительно, что 19,4% выручки от продаж решений виртуализации приходится на VDI и системы терминального доступа (данные iKS-Consulting, см. рис. 3). Это второй по объему сегмент рынка инфраструктурной виртуализации (1,93 млрд руб. в 2023 г.).

На рынке VDI, как и на рынке серверной виртуализации, лидирует «Базис» (52%, рис. 5). По сообщению компании, ее продукты используют 120 государственных информационных систем и более 700 коммерческих организаций. За 2023 г. общее количество клиентских виртуальных машин, работающих на решениях «Базиса», выросло в 7,5 раз по сравнению с 2022 г. В 2024 г. о переходе на ее экосистему объявили ВТБ и Газпромбанк. Основные конкуренты компаний на рынке VDI – ГК «Астра» и «ДАКОМ М».

Сегмент «Прочее ПО» пока занимает 5,4% рынка (см. рис. 3), но имеет хорошие перспективы для роста, прежде всего за счет бурно развивающейся контейнерной виртуализации, ежегодно увеличивающегося количества в ЕРРП решений программно определяе-



Источник: iKS-Consulting

Рис. 5. Конкурентные позиции российских игроков в сегменте решений VDI, 2023, доля выручки

мых систем хранения (SDS) и пока не представленных в реестре программно определяемых сетей (SDN). «Мы видим развитие программно определяемого ПО – SDN и SDS. Этот сегмент будет расти быстрее других направлений виртуализации, и это та точка, где мы можем не замещать импортные системы, а опережать их, т.е. создавать решения, превосходящие иностранные аналоги. В ближайшие годы совокупный среднегодовой темп роста сегмента SDN-решений составит 14%, а к 2027 г. эти решения будут занимать треть российского рынка инфраструктурных сервисов при общем его объеме более 100 млрд руб.», – дал свой прогноз генеральный директор разработ-

чика системного ПО «Базис» Давид Мартиросов.

Трудности богатого выбора

27 систем серверной виртуализации, включенных в ЕРРП, – много даже для лонг-листа. Причем число таких систем продолжает расти. Например, облачная платформа компании Cloud X (входит в En+ Group) добавлена в реестр (рег. № 25438) 12 декабря 2024 г. Эта платформа, имеющая в составе биллинг, оркестратор и решения для виртуализации серверов, систем хранения и сетей, проходит опытно-промышленную эксплуатацию на 16 предприятиях.

Также надо выбрать решения для VDI, контейнерной виртуализации, SDS и прочие продукты, обеспечивающие работу виртуальной инфраструктуры предприятия. Сложность формирования лонг-листа из множества зарегистрированных в ЕРРП систем виртуализации затрудняет российским предприятиям переход на отечественное ПО.

Частный бизнес может и должен бороться за рынок, в том числе и рынок систем виртуализации, рискнуя своими средствами, вступая в конкурентную борьбу. Тем более что рынок этот перспективный и быстро-растающий – по предварительным оценкам iKS-Consulting, в течение 2024 г. объем рынка отечественного ПО виртуализации увеличился на 42% и достиг 14,4 млрд руб. (рис. 6). Прогноз тоже благоприятный – как считают в аналитическом агентстве, до 2030 г. объем рынка будет расти со среднегодовым темпом 23,2%.

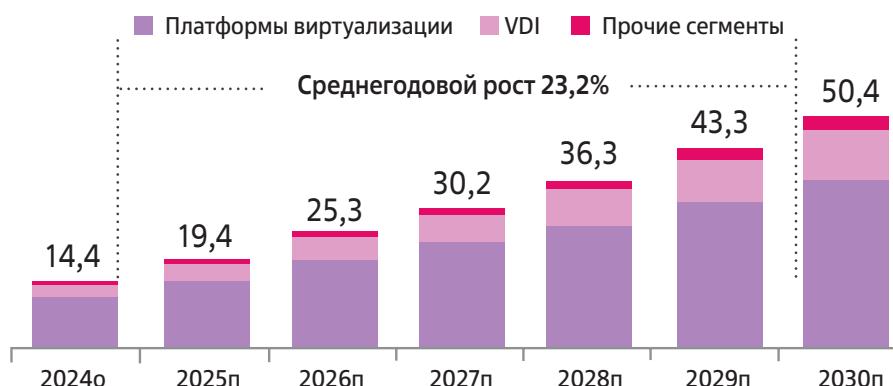


Рис. 6. Прогноз развития рынка отечественного ПО виртуализации ИТ-инфраструктуры, 2024–2030 гг., млрд руб.

Источник: iKS-Consulting

Создание множества мало отличающихся друг от друга решений за государственный счет – неэффективная трата не только денег, но и столь дефицитных сегодня человеческих ресурсов. Хороших разработчиков мало, и нет смысла заставлять их изобретать велосипед – заново писать уже существующие программы.

Но создание множества мало отличающихся друг от друга решений за государственный счет – неэффективная трата не только денег, но и столь дефицитных сегодня человеческих ресурсов. Хороших разработчиков мало, и нет смысла заставлять их изобретать велосипед – заново писать уже существующие программы. Специалистов по виртуализации не хватает, а по новым российским решениям их практически нет. Приходится переучивать айтишников, имеющих многолетний опыт работы с западными продуктами, на эксплуатацию российских решений, зачастую недостаточно зрелых. Переучиваться всегда непросто, и особенно тогда, когда в «продуктиве» все работает, а нужно переходить на решение с ограниченным функционалом и неясными перспективами, в том числе для карьеры специалиста.

Остроту проблемы можно снизить за счет главного преимущества российских компаний – близости разработчиков к заказчикам и хорошей технической поддержки. Но вендоры тоже испытывают трудности с кадрами, причем распыление ресурсов их усугубляет. «Главным сдерживающим фактором можно назвать дефицит кадров на рынке. Специалистов по виртуализации остро не хватает, к тому же они разбросаны по 40 вендорам, работающим на рынке решений для виртуализации», – указал Денис Мухин, директор департамента виртуализации и облачных сервисов ГК «Астра».

Наличие квалифицированных кадров и хорошая техподдержка – важные критерии при выборе вендора виртуализации. По сообщениям в прессе и рекламным материалам ее оценить сложно – лучше пообщаться с коллегами, уже имеющими опыт эксплуатации конкретного российского решения.

На этапе тестирования решений из шорт-листа нужно тщательно проверить их совместимость с используемыми программами и бизнес-процессами, а также работоспособность нужного функционала. «Интеграция российских продуктов с другими си-

стемами может быть сложной и требовать значительных инвестиций, что способно ограничить их распространение», – напомнил руководитель направления облачных интеграций компании «Онланта» (ГК ЛАНИТ) Кирилл Дианов.

Не стоит забывать и о безопасности. «Угрозы кибербезопасности становятся все более серьезными, и компании будут искать решения, обеспечивающие надежную защиту данных и приложений. Виртуализация может предоставить дополнительные уровни безопасности», – отметил специалист по связям с общественностью «ДАКОМ М» Шамиль Шариязданов.

И хорошо бы проработать механизмы миграции на новый продукт и пути отступления – перехода на другие решения виртуализации, если вендор ухудшит поддержку, неоправданно повысит цены или вообще уйдет с рынка. Средства автоматизации миграции на российские решения есть у большинства основных вендоров, а вот с миграцией на другие российские платформы или обратно на западные все сложнее.

На чем сердце успокоится

«В 2024 г. многие вендоры стали понимать, что создание экосистем неизбежно. Приходится объединяться, устанавливать партнерские отношения, чтобы обеспечить больше функциональных возможностей, нужных заказчику. Рынок движется к консолидации. В 2025–2026 гг. увидим на рынке двух-трех лидеров и развитые продуктные экосистемы», – считает генеральный директор vStack Евгений Карпов. С ним согласны большинство опрошенных изданием экспертов.

Многие заявляют, что стремятся стать «российским VMware», развивают продукты и расширяют экосистемы. Но российский рынок виртуализации ИТ-инфраструктуры турбулентный, все меняется быстро, и даже сегодняшним лидерам место в призовой тройке не гарантировано. Борьба идет серьезная, кто победит, непонятно, шансы есть у всех. **ИКС**

GPUaaS: что предлагают российские провайдеры

Илья Бедердинов

Федор Попко

Рынок GPU as a Service в России стремительно развивается, что соответствует глобальным тенденциям и отражает растущий интерес к облачным вычислениям в целом.

В 2023 г. объем мирового рынка GPU as a Service (GPUaaS) аналитики Global Insight Services оценили в \$5,6 млрд. Они ожидают, что в период с 2024 по 2033 гг. этот рынок будет расти на 17,6% в год и достигнет \$28,4 млрд.

Согласно данным Европейской комиссии, в 2023 г. облачными сервисами воспользовались более 45% компаний в ЕС. По сравнению с 2021 г. этот показатель увеличился на 4,2%. GPUaaS хорошо вписывается в эту динамику, обеспечивая компаниям возможность доступа к вычислительным ресурсам без необходимости покупки и эксплуатации дорогостоящего оборудования.

Российские провайдеры также в полной мере сознают высокий потенциал сегмента облачных вычислений с использованием графических процессоров. В условиях растущего спроса на вычислительные ресурсы для обработки больших объемов данных – от финансового анализа до научных исследований – GPUaaS становится ключевым сервисом на рынке ИТ-услуг. Предоставление услуг на базе GPU позволяет облачным провайдерам расширять ассортимент

сервисов в области ИИ и привлекать новых клиентов.

По нашим оценкам, в РФ облачные сервисы на базе GPU уже предлагают больше полутора десятков провайдеров, и этот список постоянно расширяется. Ниже приведена краткая информация о провайдерах, предоставивших в редакцию сведения о предлагаемых услугах GPUaaS. Будем рады получению обновленной информации, в том числе от других участников рынка, которая по мере поступления будет включаться в актуальную версию статьи на сайте «ИКС-Медиа».

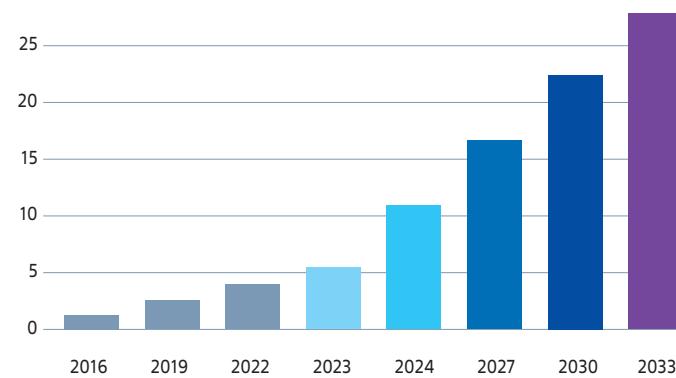
Beeline Cloud

Компания предлагает услуги IaaS с поддержкой GPU на основе собственной инфраструктуры. Пока доля GPUaaS в общем объеме ее выручки невелика, однако Beeline Cloud рассматривает эту услугу как стратегически важную для дальнейшего роста. Отказоустойчивость обеспечивается с помощью кластеров с высокой доступностью, проактивного мониторинга и резервирования необходимых ресурсов сетевой инфраструктуры.

GPUdc

Компания предлагает облачный сервис GPUaaS, используя собственный мобильный ЦОД. На эти услуги приходится значительная доля общей выручки GPUdc. Предлагается поминутная оплата, при этом пользователь может завершать аренду с сохранением состояния и в будущем продолжить работу на другом сервере.

Мировой рынок GPUaaS в 2016–2033 гг., \$млрд



Источник:
globalinsightservices.com

[сервисы и приложения]

Компания активно работает над отказоустойчивостью своих услуг, что, как отмечают ее представители, важно для клиентов, использующих GPUaaS для непрерывного запуска нейросетей в режиме 24/7. Применяются стандартные схемы обеспечения надежности, включая два независимых ввода электропитания, ИБП и резервирование сетевого оборудования. Вместе с тем представители компаний утверждают, что для большинства клиентов, использующих услуги GPUaaS для обучения нейросетей, проектирования, монтажа видео и игр, максимальная отказоустойчивость не столь принципиальна.

HPC Park

Используемая компанией платформа функционирует в собственном

GPU в сфере медиа и развлечений. Клиенты используют нейросети (LLM) для генерации текста, изображений и видео. Кроме того, увеличивается спрос на VDI-сервисы на базе GPU в контексте импортозамещения ПО класса CAD/CAE. Доля выручки от GPUaaS постоянно растет, что делает это направление стратегически важным для компании.

immers.cloud

Компания предлагает услуги GPUaaS на базе собственного ЦОДа в Москве. Тарифы на аренду GPU основаны на посекундной тарификации. Также есть скидки до 50% на долгосрочную аренду. Хотя, как отмечают в компании, отказоустойчивость менее критична для услуг GPUaaS по сравнению с классическим корпоративным обла-

и классификация объектов на видео-потоках. Эти услуги приносят immers.cloud до 90% выручки.

ITGLOBAL.COM

Инфраструктура, используемая ITGLOBAL.COM, представляет собой разновидность публичного облака на платформе VMware. Услуги с GPU составляют около 15% общей выручки компании, и она активно инвестирует в развитие этого направления.

Одна из ключевых характеристик сервисов GPUaaS, по словам представителей компании, – высокая доступность и отказоустойчивость, поскольку вычисления часто используются для задач, требующих значительных ресурсов, например, для машинного обучения и рендеринга. В случае сбоя большое количество вычислительных ресурсов окажется потраченным впустую, что может привести к значительным финансовым потерям для компаний. Отказоустойчивость провайдер обеспечивает комплексными мерами, в частности исключением единой точки отказа.

K2 Cloud

Компания K2 Cloud предлагает услуги серверов с GPU как в формате публичного облака, так и в формате HaaS, располагая собственной инфраструктурой для их предоставления. Для повышения отказоустойчивости своих услуг с GPU K2 Cloud практикует дублирование оборудования и использование кластеров. Это позволяет перераспределять нагрузку и быстро восстанавливать работу в случае сбоев с помощью резервного оборудования.

Клиенты K2 Cloud используют GPUaaS для различных задач, включая создание внутренних баз на основе генеративных моделей, разработку ИИ-агентов, например чат-ботов, а также в решениях для документооборота. Данную услугу K2 Cloud относит к стратегически важным.

MTS Web Services

Компания предоставляет услуги GPUaaS на базе собственной геораспределенной сети ЦОДов с 15 зонами доступности. Заказчики могут выби-



Есть примеры, когда для услуг GPUaaS используются системы погружного охлаждения

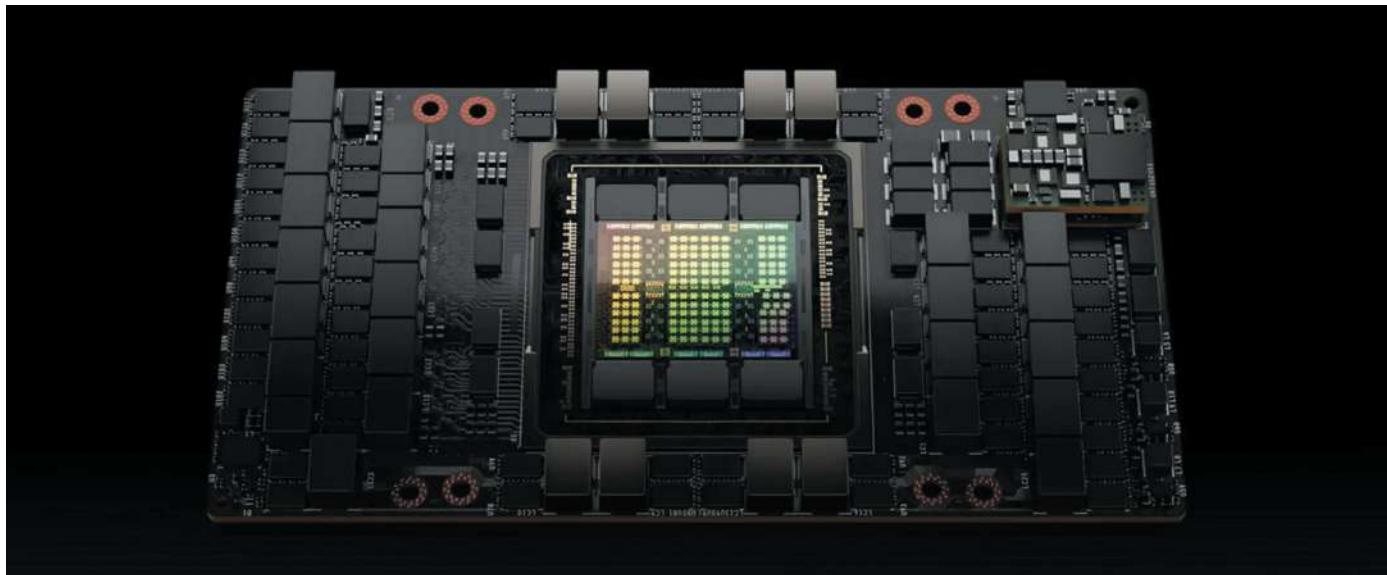
дата-центре в Москве с дублированными каналами связи и бесперебойным питанием. Пользователи GPUaaS имеют возможность через личный кабинет создавать инфраструктуру из имеющегося пулла ресурсов, включая ускорители GPU, сетевое хранилище и преднастроенное программное окружение. В настоящее время доступны серверы с GPU, а также «дробные» части этих ускорителей для менее ресурсоемких задач. Тарифы варьируются от помесячной до поминутной оплаты.

В последнее время компания отмечает рост потребления сервисов с

Увеличивается спрос на VDI-сервисы на базе GPU в контексте импортозамещения ПО класса CAD/CAE

ком, immers.cloud применяет ряд мер для повышения надежности.

Клиенты компании используют GPUaaS для решения различных задач, таких как обучение и инференс нейросетей, стриминг, сегментация



ратить из широкого спектра конфигураций на базе серверов с GPU и TPU с возможностью расширения инфраструктуры в пиковые нагрузки. Для обеспечения отказоустойчивости могут задействоваться резервные площадки.

Основные клиенты – крупные и средние предприятия, исследовательские институты, использующие GPU для анализа больших данных, прогнозирования, тестирования новых продуктов, работы с изображениями и видео, а также для биологических и медицинских исследований. Осенью 2024 г. доля услуг GPUaaS составляла 5% общей выручки компании, однако MWS видит значительный потенциал для роста этого сегмента, который ежегодно увеличивается на 40%.

Oxygen

Компания предлагает услуги GPUaaS на базе собственных data-центров. На одну виртуальную машину можно использовать до четырех карт GPU. Кластер GPU интегрирован в публичное облако и может работать совместно с другими нагрузками. При использовании профилей GPU возможно выделение части карты для виртуальной машины, что повышает устойчивость к сбоям. В обычном режиме отказоустойчивость облака также поддерживается за счет перераспределения нагрузки на другие хосты виртуализации.

Доля услуг GPUaaS в общей выручке Oxygen составляет 3–4%. Основные заказчики – компании из сфер

электронной коммерции и финтеха, а также разработчики ПО. Вместе с тем Oxygen заявляет, что спрос на эти услуги растет до 20–30% в год. В планах Oxygen – дальнейшее развитие направления, включая увеличение размера кластера с GPU.

Selectel

Провайдер предоставляет как выделенные, так и облачные серверы с GPU, а также большой запас видеокарт, модельный ряд которых регулярно обновляется. Для повышения эффективности работы с GPU клиентам предлагаются технологии Multi-Instance GPU и Time Slicing (режим разделения времени) и возможность объединения GPU через высокоскоростную шину NVLink. Возможна посуточная или помесячная оплата. По словам представителей Selectel, спрос на GPU-услуги растет, компания рассматривает их как стратегически важные и планирует развивать.

В дополнение к серверным мощностям с GPU Selectel предоставляет набор инструментов и решений для ускорения работы с задачами в области искусственного интеллекта и машинного обучения. В ML-инфраструктуру входят готовые образы для машинного обучения и анализа данных, кластеры Managed Kubernetes с GPU, работающие по принципу изоляции и автоматизации экспериментов, а также собственная платформа для обучения ML-моделей.

«Отказоустойчивость
менее критична
для услуг GPUaaS
по сравнению с класси-
ческим корпоративным
облаком»

VS

«Отказоустойчивость
особенно важна для GPUaaS,
так как вычисления часто
используются для задач,
требующих значитель-
ных ресурсов»

«Онланта»

Компания «Онланта» предоставляет серверы с GPU в формате GPUaaS на базе собственной инфраструктуры, построенной с учетом избыточности и расположенной в data-центрах уровня Tier III. В настоящее время услуги GPU приносят компании около 10% общей выручки, и эта доля постепенно растет. Тарификация предполагает помесячную оплату за виртуальные серверы с подключенной GPU-картой.

Клиенты компании «Онланта» используют GPUaaS для задач, связанных с рекомендательными системами, аналитикой и другими решениями, требующими значительных вычислительных ресурсов. В будущем компания планирует увеличивать мощности для удовлетворения растущих потребностей рынка и разрабатывать собственные продукты на базе искусственного интеллекта.

«Рег.ру»

Компания известна как поставщик физической инфраструктуры с GPU для частных облачных инсталляций (с возможностью установки оборудования на площадке клиента), а недавно запустила услугу GPUaaS. Используемые «Рег.ру» серверы позволяют установить до четырех GPU для повышения производительности. Клиенты компании передают на ее серверы с GPU задачи, связанные с дискретной обработкой массивов

данных (например, в области машинного обучения) и потоковой обработкой данных (где важна отказоустойчивость, как в случае с голосовыми помощниками и чат-ботами). Доля выручки от решений с GPU составляет около 5,4%, однако рост спроса на услуги GPUaaS компания оценивает в сотни процентов по сравнению с 2023 г., поэтому делает стратегические инвестиции в это направление. Вместе с тем в «Рег.ру» считают, что технологии TPU и FPGA в настоящее время не находят широкого применения у клиентов.



Использование облачных GPU дает значительные преимущества по сравнению с приобретением собственных серверов, включая экономию на капитальных затратах, возможность быстрого масштабирования и гибкого управления ресурсами. Клиенты могут адаптировать объем ресурсов к текущим задачам и не беспокоиться о поддержке и обновлении оборудования. Это особенно актуально для временных вычислительных задач. Модель pay-as-you-go позволяет оплачивать ресурсы по мере использования, что помогает эффективно управлять бюджетом.

Среди отраслей, активно использующих GPUaaS, выделяются ритейл, электронная коммерция и финтех. Клиенты в основном действуют

GPUaaS для следующих задач: обучение нейросетей, проектирование и моделирование, монтаж видео, анализ изображений и видеоигры.

В число доступных для клиентов графических процессоров у подавляющего большинства провайдеров входят различные модели от Nvidia. Ни один из опрошенных провайдеров не предоставляет решения на базе FPGA, и лишь одна компания предлагает решение на базе TPU. Все провайдеры акцентируют внимание на быстром росте спроса на услуги GPUaaS.

Отдельного упоминания заслуживает различное отношение провайдеров к отказоустойчивости услуг GPUaaS. Одни считают ее важной и прикладывают немалые усилия для ее обеспечения, другие отмечают, что для услуг GPUaaS отказоустойчивость менее критична по сравнению, например, с классическим корпоративным облаком. Помимо очевидного влияния специфики решаемых с помощью GPU задач причина здесь может корениваться в различиях используемой вычислительной архитектуры, в том, насколько можно сохранить промежуточные результаты и насколько велики могут оказаться потери в случае незапланированного останова.



Полный текст статьи
читайте на
www.iksmedia.ru



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

ИКС
www.iksmedia.ru

Облачные итоги – 2024. Возрождение «голого металла»

Стремление клиентов получить максимальный контроль над своими данными и низкую латентность, усилившееся с проникновением ИИ в реальный сектор экономики, привело к резкому росту востребованности услуги Bare Metal Cloud.

Антон Салов,
эксперт RCCPA

Можно сказать, что 2024-й стал в России годом Bare Metal Cloud, услуги отнюдь не новой, но продемонстрировавшей вдруг завидный рост.

Как вы услугу назовете...

Под Bare Metal Cloud (BMC) мы понимаем предоставление доступа к физическим серверам (пулу серверов), на которых отсутствуют гипервизор и операционная система. В рамках этой услуги клиент получает изолированный от других клиентов сервер или пул серверов с возможностью автоматически или самостоятельно установить ОС или развернуть систему виртуализации (классическую или K8s). По своим потребительским свойствам BMC очень близка к услугам выделенного физического сервера (относится к группе HaaS) и виртуальных вычислительных ресурсов (VPS). Однако по сравнению с ними BMC обеспечивает более широкие возможности самообслуживания при заказе, настройке (в том числе сетевых параметров), масштабировании, управлении услугой в панели или API по принципу «инфраструктура как код» (Infrastructure as code). Таким образом, BMC – более функциональная с точки зрения автоматизации услуга, чем HaaS или VPS.

По агрегированным данным зарубежных аналитических агентств, рынок Bare Metal Cloud в 2022 г. оценивался примерно в \$5 млрд, и ожидается, что в течение ближайших пяти лет он будет расти с среднегодовым темпом (CAGR) около 20%. В целом на глобальном рынке разброс оценок очень широк, что объясняется в первую очередь различиями в определении услуги BMC. Одни исследователи ограничиваются только

На глобальном рынке разброс оценок очень широк, что объясняется в первую очередь различиями в определении услуги Bare Metal Cloud

вычислительным (выделенные серверы) и сетевым (выделение, гибкая настройка и управление сетью) стеками, тогда как другие включают в оценку сервисы управления идентификационными данными (Identity Management, IDM) – синхронизацию учетных записей в приложениях, ав-

томатизацию создания и удаления учетных записей, назначение и отзыв полномочий, а также управление идентификацией и доступом (Identity & Access Management, IAM) – сервис единого входа и двухфакторной аутентификации, контроль доступа к веб-приложениям и сервисам. Некоторые исследователи расширяют охват до услуг хранения данных, включая контейнеры (K8s over Bare Metal), объектное хранение и аренду баз данных (Database Services on Bare Metal).

Кроме того, оценки различаются в отношении влияния пандемии COVID-19 на глобальный рынок Bare Metal Cloud. Так, в РФ, согласно данным iKS-Consulting, рынок BMC в 2021 г. вырос на 115% (более высокие темпы роста были только у VDI). Существенные расхождения наблюдаются и в числовых оценках негативного влияния на такие отрасли, как туризм, авиация и грузоперевозки, и позитивного – на электронную коммерцию, финансы и информационно-коммуникационные технологии. Неодинаковым было и влияние пандемии на бизнес разных размеров: в сегменте малых и средних предприятий (SMB) рост замедлился, в то время как спрос на Bare Metal Cloud в сегменте корпораций (Enterprise) активно увеличивался, что способствовало удвоению размеров рынка в относительно далеком уже 2021 г.

ВМС здесь, ВМС там

Российский рынок Bare Metal Cloud, по оценкам аналитиков iKS-Consulting, в 2023 г. достиг 10,6 млрд руб., а в 2024-м, по их же прогнозам, может составить 14,1 млрд руб., увеличившись на 33,1%. Казалось бы, это не такой уж большой сегмент IaaS в целом, да только этот пирог делят фактически четыре игрока: Selectel (56,4%), Cloud.ru (16,7%), Servers.ru (10%) и «РТК-ЦОД» (5,1%). На всех остальных (таких как EDGEЦентр и M1Cloud) в 2023 г. приходилось лишь 11,8%. Надо сказать, что только Selectel и Servers.ru явно делали упор на предоставление Bare Metal Cloud, а прочие, включая Cloud.ru, говорили, что услуга для них не фокусная, мол, предоставляем ее заказчикам по запросу, но не навязываем. Однако у Cloud.ru ВМС частично была реализована на платформе Huawei (панель управления + серверы), а частично на готовившейся к запуску собственной платформе. Кроме того, конфигурации представлялись проектные, а не типовые. В то же время у Selectel и Servers.ru все реализовано в единой панели с множеством типовых конфигураций. Например, еще в 2023 г. у Selectel было более 100 конфигураций, включая экзотические (Apple, Raspberry Pi), а у Servers.ru – около 30. Причем локации заявлялись различные. Так, у Selectel это были Москва, Санкт-Петербург, Новосибирск, Ташкент, Алматы и опять же экзотический Найроби.

Что в итоге? Небольшой, но динамично растущий сегмент (CAGR = 33,1% – это очень даже неплохо) со всеми предпосылками к дальнейшему росту (о них чуть позже), и всего четыре серьезных игрока! Причем лидер рынка Selectel активно рос именно на этой услуге и в 2024 г. дорос до третьего места в «турнирной таблице», а также до IPO (которое отложил до улучшения макроэкономической ситуации). То есть у заказчиков сформировался стабильный спрос на понятную услугу, а многие наши облачные провайдеры, включая гиперскейлеров, ее игнорируют, пытаясь выжимать соки из классического IaaS и приправляя его немножко PaaS (который всего в два раза больше ВМС).



Непорядок, решили ответственные за продуктовую стратегию и топ-менеджеры этих провайдеров, надо срочно ситуацию исправлять. И началось.

25 сентября 2024 г. Yandex Cloud на своей технологической конференции Yandex Scale сообщил о запуске (в IV квартале 2024 г. – в стадии Preview) сервиса аренды выделенных физических серверов Yandex BareMetal. «Мы увидели, что у компаний есть стабильный спрос на выделенные серверы для работы с высоконагруженными сервисами, поэтому решили запустить эту услугу», – пояснили тогда TAdviser в «Яндекс Облаке». Через пару дней о востребованности и развитии Bare Metal в России рассказал и провайдер M1Cloud: мол, не только у «Яндекса» есть ВМС, если что, заходите к нам.

Рост проникновения ИИ в реальный сектор экономики создает новый спрос на Bare Metal Cloud с GPU, так как позволяет выжать максимум из «железа» без затрат на виртуализацию

Месяцем позже, тоже 25 числа, другой отечественный гиперскейлер, Cloud.ru, заявил, что теперь и у него есть Bare Metal, но уже не от Huawei, а на базе собственной платформы Cloud.ru Evolution, т.е. импортозамещенный, как и у остальных. Говорилось о рекордном времени прошивки сервера после заказа

(менее 1 мин, но без учета времени на установку операционной системы). Для ВМС это очень важный параметр. Декларировалась также поддержка управления сервером через VNC-консоль в личном кабинете либо через API. Про поддержку Terraform не сказали (у EDGEЦентра и Servers.ru такая возможность есть, Selectel анонсировал в октябре 2024 г. на Selectel Tech Day, до этого не было).

VK Cloud, также претендующий на звание гиперскейлера, особенно в свете своих планов дальнейшего строительства сети ЦОДов, ВМС как продукт на рынок не вывел, но заявляет: «Если вы предпочитаете Bare Metal для максимального контроля над своими кластерами и выполнения специфичных требований к безопасности, мы готовы дать вам продвинутый сервис для размещения на выделенных серверах». В общем, пока это не продукт, а проектный подход. Но он есть, а значит, вероятно, скоро увидим такой продукт от VK Cloud. Благо провайдер не упирается исключительно в модель AWS и активно строит и частные облака, и задействует модель облачной интеграции с коллегами по VK Tech. Просто, по нашим данным, перед менеджментом пока стояла задача навести порядок в существующем продуктовом портфеле, а не нарастить функциональность.

Что же такого произошло, спросите вы, что рынок вдруг вспомнил про Bare Metal Cloud, где же все эти 40 систем отечественной виртуализации, которые включены в реестр отечественного ПО? Все хорошо с классическими облаками и с класси-



ческой виртуализацией, да и с контейнерной тоже. Разберемся, почему услуга стала так популярна, и сначала посмотрим на глобальный рынок.

На западном фронте

Среди западных гиперсейлеров есть IBM Cloud, он же Bluemix, который основывается на купленном крупнейшем провайдере выделенных серверов Softlayer. В глобальной структуре доходов IBM Cloud BMC занимала более 40%, а в РФ вроде бы даже больше. Для чего использовалось облако IBM? В первую очередь для финансовых операций: высокочастотная торговля и обработка финансовых данных требуют минимальной задержки, и Bare Metal Cloud может обеспечить более низкую латентность по сравнению с виртуальными средами. Мейнфреймы IBM продолжают безотказно трудиться во множестве финансовых институтов, и альтернативой им может стать только кластер BMC. IBM в рамках IBM Cloud активно предлагает услугу IBM Cloud Bare Metal Servers с консалтингом по переносу операций с мейнфреймов и интеграцией с классическими облачными сервисами, такими как IBM Watson.

Параллельно началась деклаудизация, в которой во многом виновата Broadcom. Она так перекроила схему лицензирования VMware после M&A, что «жуткий вой на болотах», начавшийся в 2023 г., не утих и в 2024-м, о чем я писал в итогах 2023 г. С тех пор было несколько послаблений, но проблему они не решили. Отказ от пожизненных лицензий был воспринят клиентами очень болезненно. В сентябре американский телекоммуникационный гигант

AT&T даже подал иск к Broadcom (правда, спустя два месяца стороны вопрос урегулировали). Президент Broadcom Хок Тан оправдывал свои действия попыткой упростить схему лицензирования и близорукостью оппонентов, которые купили бессрочные лицензии и не думают об их амортизации. Но эти оправдания не нашли отклика. Те, кто не хотел идти к глобальным гиперсейлерам, а предпочитали держать свои данные у себя (особенно в Европе), стали рассматривать альтернативы. А их не так уж и много, у них ведь нет 40+ систем виртуализации, как у нас.

Готовить BMC тоже надо правильно. Если вы заявляете BMC, то готовьтесь к быстроте провиженинга и автоматизации настроек

А тут еще и хайп на ИИ. Модели надо тренировать на своих данных, которые мало кто из крупных корпораций хочет отдавать облачным провайдерам, и для этих целей Bare Metal Cloud подходит как нельзя лучше. Рост проникновения ИИ в реальный сектор экономики создает новый спрос на Bare Metal Cloud с GPU, так как позволяет выжать максимум из «железа» без затрат на виртуализацию.

А у нас?

Но у нас почему бум произошел именно в 2024 г.? Во-первых, как пел Чиж, «до нас все всегда доходит с опозданием в несколько лет». Развитие

российского рынка всегда отставало от западных ИТ-тенденций, хотя и не во всем. Во-вторых, полномасштабное детальное исследование рынка BMC, проведенное iKS-Consulting в конце 2023 г., показало его большой потенциал. В-третьих, заявка Selectel на IPO и покупка провайдером актива из топ-3 этого сегмента рынка (100% акций ООО «Единая сеть», которое работает под брендами Servers.ru, E xepto.ru и Fozzy.ru) убедили всех в перспективности данного направления. И даже те, кто до этого смотрел на BMC свысока и называл недокладом, срочно стали перекраивать свои продуктовые планы.

Однако готовить BMC тоже надо правильно. Не только воткнуть серверы в стойку и подключать по запросу, это не облако. Если вы заявляете BMC, то готовьтесь к быстроте провиженинга и автоматизации настроек. Если используется кластер и несколько стоек, провайдер Bare Metal Cloud должен предложить управление правилами совместного (affinity) или раздельного (anti-affinity) размещения серверов в одной стойке, локации ЦОДа или же в разных. Для ряда сценариев это может быть критично. У провайдера BMC должна быть возможность настраивать правила и политики в панели управления, через Terraform или через API. В общем, заявить услугу – это одно, а сделать ее настолько классной для клиентов, чтобы тебя захотели купить IBM или Selectel – совсем другое.

Кстати, помимо финансистов с их комплаенсом и владельцев legacy-софта, который просто не работает в среде виртуализации, потому как создан в то время, когда про cloud ready никто и не слышал, Bare Metal Cloud очень любят наши провайдеры услуг класса SaaS. У них есть своя DevOps-команда (или хороший аутсорсинг), они умеют готовить идеальную конфигурацию под свои типовые нагрузки, хорошо понимают, когда происходят всплески нагрузки, и выжимают из «железа» оптимум, прилично при этом экономя. Поэтому классический IaaS или Managed Kubernetes им не нужны. Да и «кубер» отлично живет поверх BMC. **ИКС**

Карты таро и другие способы оценки рынка информационной безопасности

Объем рынка – важный показатель, помогающий компаниям и инвесторам прогнозировать рост и принимать стратегические решения. Но его противоречивые оценки вызывают вопросы к используемым аналитиками методикам.



Николай Носов



Запрос на аналитику

Как оценить объем рынка? Этот вопрос интересен не только гигантам бизнеса, готовящимся к IPO, но и небольшим компаниям – для планирования своей деятельности. Самый простой способ получить ответ – посмотреть оценку мирового рынка, сделанную авторитетными аналитическими агентствами, а потом взять от нее 2% (долю России в мировой экономике). Например, мировой рынок кибербезопасности в 2024 г. Mordor Intelligence оценивает в \$203,78 млрд (рис. 1). Соответственно объем российского рынка составит 406 млрд руб. – цифра, не вызывающая резкого отторжения.

Таким образом можно получить грубую оценку, но именно грубую,



Период исследования	2019–2029
Размер рынка (2024)	\$203,78 млрд
Размер рынка (2029)	\$350,23 млрд
CAGR (2024–2029)	11,44%
Самый быстрорастущий рынок	Азиатско-Тихоокеанский регион
Самый большой рынок	Северная Америка

Источник: Mordor Intelligence

Рис. 1. Глобальный рынок кибербезопасности

приближенную, поскольку в одних областях Россия отстает от мирового уровня, в других, например в той же кибербезопасности, существенно его опережает. Если нужна более точная оценка, стоит обратиться к аналитическим агентствам: конечно, не к произвольно выбранным, а к тем, которые хорошо знают исследуемый рынок, накопили по нему большую экспертизу и объемы не всегда публичных данных.

Методы оценки

Обычно при оценке объема рынка аналитики используют методы «сверху вниз» и «снизу вверх». Метод «сверху вниз» предполагает оценку рынка на основе общих данных и тенденций, в то время как метод «снизу вверх» основывается на анализе конкретных данных о потреблении и продажах.

«При оценке объема рынка важно зафиксировать таксономию рынка (его структуру и набор сегментов и продуктов, которые мы в этот рынок включаем), – говорит ведущий консультант iKS-Consulting Станислав Мирин. – Базу оценки объема и прогноза динамики составляет анкетирование участников рынка с дроблением на отдельные подсегменты. Ответы сопоставляются с объемами выручки компаний по данным Росстата, рассчитываются производные показатели. Например, для ЦОДов мы проверяем доход на стойко-место и среднюю площадь под одну стойку, которые в целом по рынку, как правило, сопоставимы. А если есть существенные отличия, запрашиваем пояснения участников. Суммируем данные по нескольким десяткам крупнейших участников рынка и получаем оценку объема рынка ЦОДов «снизу вверх».

Одновременно оцениваем динамику спроса: количество клиентов и

Таксономия рынка кибербезопасности

Категории	Средства
Средства защиты инфраструктуры (Infrastructure security)	<ul style="list-style-type: none"> ■ Средства управления событиями ИБ (Security Information and Event Management, SIEM) ■ Средства анализа киберугроз (Threat Intelligence, TI) ■ Средства оркестровки (управления) систем безопасности (Security Orchestration, Automation and Response, SOAR) ■ Средства защиты промышленных систем управления (систем управления технологическими процессами) (Industrial Control System (ICS) security) ■ Платформа реагирования на инциденты (Incident Response Platform, IRP) ■ Платформы управления рисками (Governance, Risk and Compliance, GRC).
Средства защиты сетей (Network security)	<ul style="list-style-type: none"> ■ Межсетевые экраны (Firewall), в том числе нового поколения (Next Generation Firewall, NGFW) ■ Многофункциональные решения (Unified Threat Management, UTM) ■ Системы обнаружения/предотвращения вторжений (Intrusion Detection/Prevention System, IDS/IPS) ■ Системы анализа трафика (Network Traffic Analysis, NTA) ■ Средства контроля доступа к сети (Network Access Control, NAC) ■ Средства защиты от сложных и неизвестных киберугроз (Network Detection & Response, NDR) ■ Шлюзы информационной безопасности (Security Web/Mail Gateway, SWG/SMG) ■ Сетевые «песочницы» (Network Sandbox) ■ Виртуальные частные сети (Virtual Private Network, VPN).
Средства защиты приложений (Application security)	<ul style="list-style-type: none"> ■ Средства контроля и оценки уязвимостей (Vulnerability Assessment, VA) ■ Средства управления уязвимостями (Vulnerability Management, VM) ■ Средства поиска уязвимостей в исходном коде ПО (Application Security Testing, AST) ■ Межсетевые экраны для веб-приложений (Web Application Firewall, WAF) ■ Средства защиты от DDoS-атак (DDoS Protection).
Средства защиты данных (Data security)	<ul style="list-style-type: none"> ■ Средства защиты от несанкционированного доступа (Unauthorized Access Protection, UAP) ■ Средства защиты от утечек информации (Data Loss Prevention, DLP) ■ Средства шифрования (Encryption).
Средства защиты пользователей (User security)	<ul style="list-style-type: none"> ■ Средства управления идентификацией, аутентификацией и контроля доступа (Identity & Access Management/Governance & Administration, IAM/IGA) ■ Средства контроля привилегированных пользователей (Privileged Access Management, PAM) ■ Средства криптографической защиты информации пользователей, в том числе средства электронной подписи (Public Key Infrastructure, PKI).
Средства защиты конечных точек (Endpoint security)	<ul style="list-style-type: none"> ■ Средства антивирусной защиты (Antivirus Protection, AVP) ■ Системы обнаружения и реагирования на угрозы на рабочих станциях пользователей (конечных точках) (Endpoint Detection and Response, EDR).

Источник: ЦСР



среднюю выручку на одного клиента (ARPU). Учитываем факторы, влияющие на развитие рынка, общее состояние экономики, инфляцию, различные случайные факторы и их вероятность. Смотрим на тренды развития отечественного рынка предыдущих лет и динамику аналогичных зарубежных рынков. Таким образом получаем оценку рынка в целом и дальше на основе осредненных данных из анкет и интервью дробим ее по различным подсегментам, регионам и стратам клиентов (оценка “сверху вниз”). В идеале эти две оценки должны сходиться».

Проблемы таксономии

Определение границ рынка – первый и очень важный этап анализа, основная причина разброса оценок аналитиков. В исследованиях Mordor Intelligence изучался рынок кибербезопасности, включающий доходы как вендоров, так и компаний, предлагающих услуги. В чаще всего цитируемых оценках российского рынка кибербезопасности, сделанных фондом «Центр стратегических разработок» (ЦСР), учтены только доходы вендоров решений по защите инфраструктуры предприятий. В 2023 г., по данным ЦСР, этот рынок составил 248 млрд руб.

С услугами сложнее. Из оценок крупных сегментов в публичном пространстве доступна оценка рос-

сийского рынка центров мониторинга и реагирования на инциденты (SOC) и провайдеров услуг ИБ (MSSP) от аналитического агентства iKS-Consulting – 22,9 млрд руб. в 2023 г. Суммируя с доходами вендоров, получим 270,9 млрд руб., что уже сопоставимо с оценкой, приведенной в начале статьи (365 млрд руб. в пересчете на 2023 г. при CAGR = 11,44%). А ведь в сферу услуг входят еще обучение и консультации, поддержка и обслуживание, проектирование и интеграция.

По доходам вендоров картина тоже не исчерпывающая. В проведенном ЦСР исследовании «Прогноз российского рынка кибербезопасности в Российской Федерации на 2023–2027 гг.» анализировались только шесть категорий защиты (см. таблицу).

Сразу можно сказать, что список категорий неполон. В нем нет средств защиты разработки программного обеспечения (DevSecOps), в которые входят: средства тестирования приложений на этапе разработки с применением техники статического анализа (Static Application Security Testing, SAST); средства проверки программ в рабочем состоянии для поиска уязвимостей методом «черного ящика» (Dynamic Application Security Testing, DAST); средства проверки на известные уязвимости и зависимости программ с откры-

тым исходным кодом (Open Source Analysis, OSA).

Не охвачена облачная безопасность (Cloud Security) – набор инструментов, ориентированных на защиту облачной инфраструктуры. В этот набор входят, в частности, брокеры безопасности облачного доступа (CASB); платформы защиты облачных рабочих процессов (CWPP); системы управления состоянием облачной безопасности (CSPM).

Непонятно, как учитываются решения для мониторинга внешних киберугроз (DRP) и защиты бренда (Brand Protection), и не оценивается специфичный рынок СОРМ. Кроме того, в анализируемый рынок не попали сканеры уязвимостей, используемые для оценки защищенности инфраструктуры, услуги пентестеров и платформы Bug Bounty. Возможно, вклад этих направлений в общую картину невелик, их можно объединить в категорию «Другие средства» и не учитывать в итоговой цифре. Но эту гипотезу нужно проверить.

Для полноты картины было бы неплохо изучить и рынок B2C, доля которого в общем рынке кибербезопасности России может оказаться заметной. Во всяком случае я сам ежегодно плачу за домашние лицензии на антивирус. Пусть сумма скромная, но и физических лиц намного больше, чем компаний.

Зачем нужны оценки рынка

Список анализируемых категорий во многом зависит от задач, стоящих перед исследователями. Аналитиков вендоров в первую очередь интересуют сегменты, в которых представлены продукты компании. «Первая наша цель – оценить, сколько заработкаем в ближайшем будущем», – заявил технический директор компании Avanpost Александр Махновский на прошедшей в рамках SOC Forum 2024 дискуссии «Тайная жизнь цифр ИБ». «В первую очередь [оценки рынка нужны] для стратегического планирования и постановки целей по продажам», – поддержала коллегу директор по стратегическому управлению «Лаборатории Касперского» Илона Раппу. Кроме того, на доле рынка и на понимании, насколько рост выручки соответствует росту в рыночном сегменте, стране или регионе, основывается оценка эффективности продаж.

Вендоры задействуют оценки для анализа сегментов, на которые планируют выводить новые продукты: есть ли свободные ниши, какова в них конкуренция, какой прогнозируется рост. Цифры аналитиков используются для выбора перспективных продуктовых линеек, планирования инвестиций, составления плана продаж для продавцов и прогноза выручки для акционеров (рис. 2).

«Нам интересна оценка не всего рынка ИБ, а отдельных решений и трендов развития», – отметил руководитель департамента развития бизнеса решений ИБ компании Axoft Никита Черняков. Например, ком-

пания показывает партнерам, что на определенном отрезке времени увеличивается использование того или иного решения, и предлагает в него инвестировать.

Консультантам и аналитическим компаниям интереснее оценки рынка в целом. «Мы как консультанты пользуемся аналитикой, чтобы формировать стратегии для заказчиков, показывать работающим в смежных отраслях клиентам, что ИБ – привлекательный рынок», – пояснил ассоциированный партнер ГК Б1 Сергей Салов.

Аналитика рынка, как уточнила заместитель генерального директора ЦСР Екатерина Кваша, требуется компаниям, планирующим IPO, выходящим на новые рынки или расширяющим свое присутствие на старых. Кроме того, в аналитике заинтересованы госорганы, которым нужны оценки процессов, происходящих в стране. Например, им важно знать, как проходит импортозамещение, есть ли российские вендоры в том или ином сегменте и какие позиции они занимают.

Сложности анализа

Для оценки рынка нужны данные, но получать их после 2022 г. стало намного сложнее. Раньше было проще – лидировавшие на российском рынке зарубежные вендоры публиковали отчетность о продажах по регионам, многие цифры можно было проверить по данным таможни, не было так трудно считаемого параллельного импорта и такого большого числа подсанкционных компаний, не стре-

мящихся афишировать достижения своего бизнеса.

Немного проще аналитикам интеграторов – они по своим клиентам видят суммы, потраченные на те или иные категории средств защиты и продукты, и могут экстраполировать их на рынок в целом, оценивая этот рынок в деньгах клиентов. С другой стороны, они ограничены продаваемыми продуктами, поэтому видят только часть рынка, да и погрешности при экстраполяции могут быть существенными.

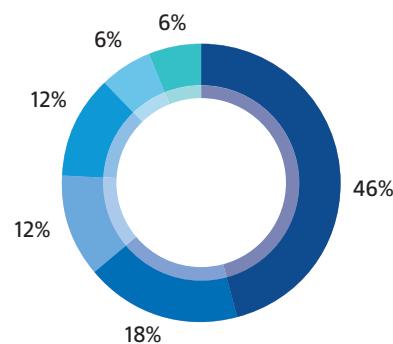
Аналитическим компаниям приходится опираться на официальные, но очень высокоуровневые цифры Росстата, разбивая общие оценки на выручку по категориям путем анкетирования компаний. А с этим тоже непросто – если у компании есть чем похвастаться и она чувствует себя в лидерах сегмента, то данные дают. Если же нет – зачем ей к этому привлекать внимание? Для оценки таких компаний приходится использовать сторонних экспертов и косвенные данные – аудиторские отчеты, пресс-релизы, опросы на пресс-конференциях и инсайд.

Тема информационной безопасности специфичная, мало кто готов раскрывать цифры. «Мы знаем вендоров, которые присутствуют на рынке, продукты, которые они продают, и идем от выручки вендоров, не перепроверяя через заказчиков, что бессмысленно в текущей ситуации, когда часть тендеров закрыта», – пояснила Е. Кваша. При этом ЦСР все же



Рис. 2. Как игроки рынка ИБ в первую очередь используют данные о рынке

- Цели по продажам
- Оценка конкурентности
- Привлечение инвесторов
- Разработка инноваций
- Развитие отрасли
- Другое



Источник: Опрос на SOC Forum 2024

перепроверяет цифры, например, с помощью экспертных оценок. А вендоры могут связаться с аналитиками и обсудить получившиеся результаты.

И раскинет она и разложит

Формируя прогноз развития российского рынка, можно ориентироваться на темпы роста мирового. По оценке аналитиков Expert Market Research, глобальный рынок кибербезопасности в 2023–2028 гг. будет увеличиваться в среднем на 8,7% в год. Mordor Intelligence для периода 2019–2029 гг. дает CAGR = 11,44%. Близкую к этим цифрам – 10–15% – оценку темпов роста российского рынка высказали в ходе дискуссии вендоры и слушатели в зале. Но аналитики смотрят в будущее более оптимистично. Так, TAdviser оценивает рост рынка в 2022–23 гг. в 25%, а ЦСР считает, что CAGR за период 2022–2027 гг. составит около 24%.

Российские аналитики считают в рублях и, как правило, учитывают базовый прогноз ЦБ РФ по инфляции (примерно 4%), но тем не менее оценки впечатляют. Для реального роста есть все основания. Один из фундаментальных драйверов рынка информационной безопасности – процессы цифровизации. Рынок ИБ можно рассматривать как часть рынка ИТ, во всяком случае именно такой подход использует аналитическое агентство Strategy Partners, оценивая мировой рынок ИБ как 10% рынка ИТ (рис. 3). Связь есть – чем больше компьютеров и программ, тем больше требуется средств защиты. На цифровизацию накладывается еще один мощный драйвер, особенно актуальный для России, – стремительный рост количества, масштаба и сложности кибератак, приводящий к дополнительному перераспределению средств из ИТ в целом в ИБ.

Другой важный драйвер роста российского рынка – импортозамещение. Одни компании по своей инициативе отказываются от продуктов ушедших с рынка западных игроков, лишившись их поддержки, другие делают это под давлением регулятора. Так или иначе деньги выделяются, и рынок растет. Снижается основной барьер – не-

дооценка угроз. Касающийся всех граждан и компаний кибертерроризм заставил перейти от бумажной безопасности к реальной, причем во всех сферах. Как отметила И. Раппу, в этом году «Лаборатория Касперского» наблюдает резкий рост рынка в секторе СМБ. И пусть там используют более дешевые решения, зато таких компаний много.



Оценка рынка ИБ, млрд руб.

	2023
Strategy Partners (10% от рынка ИТ)	310
ЦСР	248
«СТРИМ Консалтинг»	235
Statista	216
Сценарии из интернета	317

Источник: SOC Forum 2024

Рис. 3. Оценка рынка ИБ аналитиками

Однако санкции – барьер, который продолжает действовать. Он особенно сказывается на закупке зарубежных аппаратных средств защиты. Хотя не все компании чувствительны к рискам недекларированных возможностей иностранного оборудования, сложности расчетов и поставок уменьшают возможности покупки зачастую существенно более дешевых зарубежных аппаратных и программных средств.

Препятствует развитию рынка и высокая ставка рефинансирования, ограничивающая использование за-

емных средств для закупки решений информационной безопасности.

«При прогнозировании рынка кибербезопасности учитываются драйверы, барьеры, планы компаний и используется экспертная оценка вероятности их выполнения, – пояснил ведущий консультант iKS-Consulting Максим Савватин. – Анализируется средняя выручка на клиента в зависимости от масштаба компании (крупное предприятие, СМБ), изменение размера клиентской базы (рост числа клиентов из СМБ), требования регуляторов и степень их выполнения, макроэкономические показатели, в том числе уровень инфляции. Важно учитывать динамику по сегментам, так как для разных продуктов она может существенно различаться.

Стоит присматриваться к зарубежным прогнозам динамики отдельных направлений. Любой прогноз вероятностный – помимо непредсказуемых «черных лебедей» и неожиданных крупных госзаказов существует разброс оценок экспертов, причем чем на больший срок делается прогноз, тем разброс больше. Но все же прогноз дает определенную точку опоры, на нем можно строить планирование, а это уже немало».

Стоит отметить и эффект «самоиспользующегося прогноза». Если рынок верит, что у сегмента есть хорошие перспективы, то станет в него инвестировать, и он действительно будет расти. Так что прогнозы могут не только оценивать будущее, но и влиять на него.

В первоначальном варианте дискуссия о цифрах на SOC Forum 2024 должна была завершиться гаданием о будущем рынке кибербезопасности на картах таро. Времени не хватило, а жаль. В каждой шутке есть доля правды. Как прогноз на картах таро зависит от аркана выпавших карт, так и прогноз аналитиков – от собранной о рынке информации. Но окончательный вариант определяется опытом аналитика-гадалки, его пониманием рынка, тенденций и ожиданий, а также вопросами, которые ставит клиент. **ИКС**

Оценка рисков информационной безопасности: сколько вешать в граммах?

Дмитрий Костров

заместитель генерального директора по информационной безопасности, «ИЭК Холдинг»

Угрозы информационной безопасности, которые нередко влияют на непрерывность бизнеса и даже на само его существование, стали, увы, обыденной проблемой. Поэтому так важно своевременно оценивать соответствующие риски, причем оценку давать количественную, «в граммах».

Проблема оценки рисков информационной безопасности не нова. Многие компании, особенно ведущие бизнес, который сопряжен с риском, применяют риск-ориентированный подход и в сфере информационной безопасности. При этом, если мы говорим о «чисто бизнесе», владельцы компаний требуют не качественную оценку, а именно количественную, что вовлекает в процесс все бизнес-подразделения организации.

Здесь уместно процитировать Стивена Холта, видного безопасника, занимающего пост ИТ-директора Materion Corporation: «Когда ваша организация подвергнется кибератаке, которая приведет к потере данных, сбоям в работе систем и репутационному ущербу, – это лишь вопрос времени. Кибербезопасность – уже не просто технологическая проблема, а проблема бизнеса». Это правда. И риски информационной безопасности – проблема не только ИБ-подразделения, а всего бизнеса компании. Поэтому и оценивать такие риски должен не только отдел ИБ, но и руководители бизнес-единиц по предложенной этим подразделением методике.

И еще одно мотивирующее высказывание, которое приписывают Рэнди Стейнбергу, гуру в области ITSM: «Если вы не измеряете процесс, вы не сможете им управлять. Если вы не измеряете процесс, вы не сможете его улучшить. Если вы не измеряете процесс, вам, вероятно, нет до него дела». Это все к тому, что каким бы муторным ни был процесс оценки рисков, его надо проводить.

Что даст оценка рисков?

Оценка рисков ИБ служит основой формирования дополнительных преимуществ для бизнеса, способствуя повышению уровня киберустойчивости компании, снижению затрат на устранение последствий реализации рисков. Кроме того, она позволяет:

- выявить слабые места и системные проблемы в ландшафте средств обеспечения безопасности и ИТ;
- снизить вероятность реализации информационных угроз, обеспечить непрерывность бизнеса;
- повысить текущий уровень защищенности ИТ-сервисов и инфраструктуры;

- определить вектор развития, выявить способы и ресурсы для повышения зрелости ИБ в компании;
- снизить вероятность возникновения финансовых, репутационных, клиентских и регуляторных рисков;
- сформировать базу для дальнейшего развития корпоративного подхода к обеспечению безопасности.

Оценка рисков ИБ – это проект. Давайте уточним, что нужно сделать в рамках этого проекта.

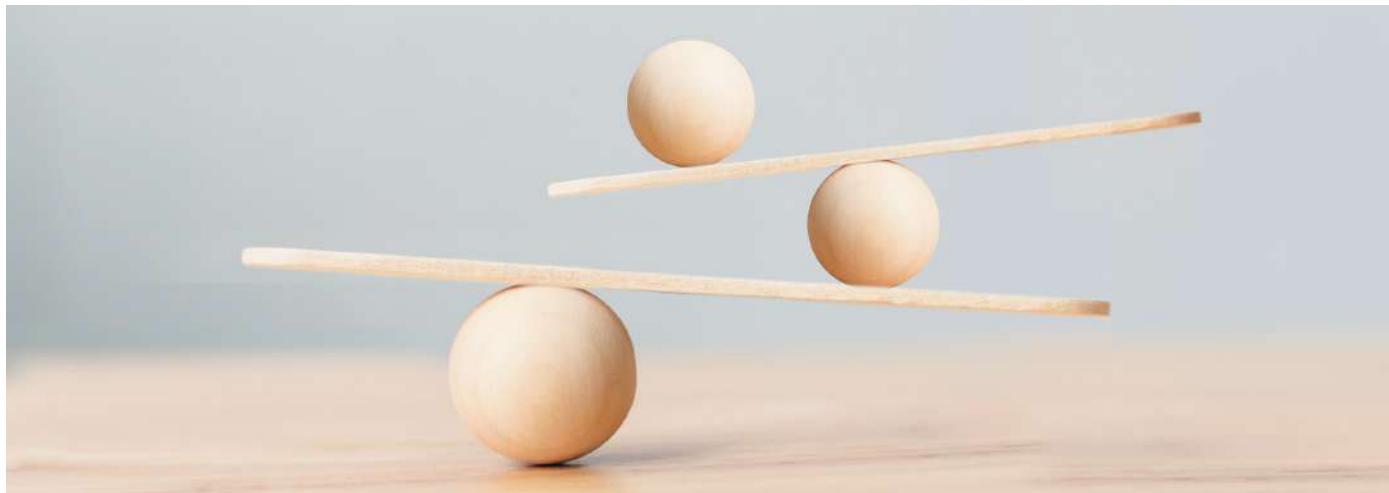
Порядок оценки рисков

Прежде всего, на подготовительном этапе, нужно уточнить и зафиксировать границы обследования и цели работ, составить план-график работ, подготовить опросные листы и изучить полученные ответы, провести интервью с ключевыми представителями бизнес-подразделений.

Кроме того, следует проанализировать используемые в компании подходы к управлению ИБ, изучить полноту и корректность имеющихся документов в области ИБ, оценить состояние ключевых ИБ-процессов и их характеристики, разработать базу рисков ИБ (далее вместо «риски ИБ» будем в большинстве случаев писать просто «риски»).

Затем предпринимают следующие шаги:

- определяют бизнес-процессы, включаемые в анализ, уровни критичности бизнес-процессов и основных информационных систем (ИС), критерии принятия риска;
- идентифицируют актуальные риски, определяют возможные причины



(источники) их возникновения, категории потенциального ущерба и виды последствий от реализации рисков, разрабатывают шкалы влияния рисков по категориям ущерба и шкалы вероятности реализации рисков;

- проводят анализ рисков: оценивается влияние каждого выявленного риска по каждой из категорий ущерба, вероятность реализации рисков с учетом состояния контрольной среды компании, внутренних и внешних факторов; рассчитывается потенциальный ущерб от реализации рисков; делается индивидуальная оценка каждого риска и оценка их интегрального уровня;
- оценивают возможность принятия каждого риска, рассматривают варианты обработки рисков; планируют мероприятия по обработке рисков; определяют владельцев рисков ИБ и ответственных за мероприятия по обработке рисков.

Такая оценка рисков может осуществляться как на периодической основе, так и по указанию руководства.

Действующие лица и исполнители

Оценка рисков проводится членами комитета по управлению рисками ИБ (КУРИБ), в который должны войти представители ИБ-, ИТ- и, самое главное, бизнес-подразделений. Часто оценку рисков возлагают на комитет по ИБ (КИБ), что не совсем правильно.

КИБ – постоянно действующий коллегиальный орган компании и составная часть ее системы управ-

ления информационной безопасностью (СУИБ). А СУИБ, в свою очередь, – часть общей системы менеджмента компании, которая на основе риск-ориентированного подхода занимается созданием, реализацией, эксплуатацией, мониторингом, анализом, поддержкой и совершенствованием информационной безопасности компании. В КИБ обычно входят руководители подразделений ИБ и ИТ, генеральный директор, исполнительный директор и приглашенные эксперты.

КУРИБ, исходя из перечня входящих в область оценки бизнес-процессов компании, составляет реестр поддерживающих непрерывность этих бизнес-процессов информационных систем и определяет наиболее критичные ИС, которые будут включены в область оценки. Наиболее критичными признаются ИС, недоступность которых негативно влияет на бизнес-процессы компании и может привести к остановке ее деятельности, финансовым и репутационным потерям, потере клиентов или сделок, санкциям со стороны государственных регулирующих органов.

Ход процесса оценки рисков документирует специальный сотрудник – менеджер рисков ИБ.

Методика оценки

Методика разрабатывается с учетом контекста компании, экспертной оценки актуального уровня ИБ, требований внутренней документации,

Если вы не измеряете процесс, вы не сможете им управлять.

Если вы не измеряете процесс, вы не сможете его улучшить.

Если вы не измеряете процесс, вам, вероятно, нет до него дела.

отраслевого опыта подрядчика и положений ключевых стандартов в области ИБ, а именно:

- ГОСТ Р ИСО 31000-2019. Менеджмент риска. Принципы и руководство.
- ГОСТ Р ИСО/МЭК 27001-2021. Системы менеджмента информационной безопасности. Требования.
- ГОСТ Р ИСО/МЭК 27002-2021. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности.
- ГОСТ Р МЭК 31010-2021. Надежность в технике. Методы оценки риска.

Методика должна базироваться на экспертном анализе, когда идентификация потенциальных рисков, оценка их причин, вероятности реализации этих рисков и возможного ущерба делается на основе мнения коллектива специалистов, их профессиональных знаний и практического опыта, а также учета специфики бизнеса компании.

Экспертная оценка формируется путем мозгового штурма (brainstorming) и использования техники анализа опасности и работоспособности (hazard and operability study, HAZOP). Мозговой штурм применяется на всех этапах управления рисками ИБ в ходе коллегиального обсуждения связанных с рисками аспектов. Он предполагает свободное обсуждение внутри группы хорошо осведомленных сотрудников компании – экспертов в различных областях ее деятельности и учет мнений участников. Техника HAZOP задействуется на этапе анализа рисков, когда участники процесса формулируют последствия и оценивают потенциальное воздействие идентифицированных рисков на способность компании достигать бизнес-целей, определяют возможные причины идентифицированных рисков и вероятность их реализации. HAZOP предполагает моделирование рисков ИБ, их причин и последствий, а также дальнейшую оценку полученных моделей в корпоративных терминах, с применением соответствующих критериев или шкал.

Собственно процесс

Итак, КУРИБ составляет перечень бизнес-процессов компании, включаемых в область оценки рисков, и определяет уровень критичности каждого из таких бизнес-процессов, исходя из уровня влияния прерывания бизнес-процесса на финансовые показатели компании с использованием специальной шкалы.

Например, выбираются три уровня критичности бизнес-процессов:

Низкий. Сюда относятся наименее критичные процессы. Возможное воздействие риска ИБ для компании приемлемо. Ключевые бизнес-операции будут затронуты незначительно.

Если в ходе оценки члены КУРИБ определили различные уровни ущерба для одного и того же риска, должен быть принят наихудший сценарий и в реестре зафиксирована самая высокая оценка

Средний. Умеренно критичные процессы. Возможное воздействие риска в целом для компании приемлемо. Выполняемые бизнес-операции будут заметно затронуты, включая возможное нарушение некоторых договорных обязательств. Возможны также умеренный отток клиентов и умеренное снижение доходов/увеличение расходов.

Высокий. Наиболее критичные процессы. Возможное воздействие риска ИБ для компании крайне нежелательно. Выполняемые бизнес-операции будут затронуты существенно, включая возможные нарушения правовых, нормативных или договорных требований либо потерю доверия общественности к бренду

компании. Возможен значительный отток клиентов, упущенная выгода либо косвенное негативное влияние, ведущее к существенному снижению доходов/увеличению расходов.

На основе определенных уровней критичности каждому бизнес-процессу из области оценки присваивается коэффициент критичности по следующей шкале: 1 для высокого уровня критичности, 0,75 для среднего и 0,5 для низкого. Коэффициент критичности документируется менеджером рисков в поле «Коэффициент критичности» специального реестра.

Далее КУРИБ путем мозгового штурма, а также с учетом результатов предыдущей оценки рисков (если такая проводилась) определяет перечень рисков, могущих потенциально влиять на непрерывность бизнес-процессов компании из области оценки. Идентифицированные риски фиксируются менеджером рисков в специальном реестре и заполняются соответствующие поля: «Тип риска ИБ», «Вид риска ИБ», «Описание риска ИБ», «Возможные причины риска ИБ».

Реализация риска ИБ может привести к различного рода последствиям, в том числе к сбоям в работе ИС, прерыванию бизнес-процессов, нарушению доступности, конфиденциальности и целостности корпоративных данных и т.д., иными словами, причинить компании ущерб того или иного характера. КУРИБ устанавливает период прерывания функционирования ИС, в отношении которого определяется потенциальный ущерб. По умолчанию период прерывания равняется 8 рабочим часам (1 рабочему дню). Также применяется время простоя (например, склада): час, день, неделя.

Затем КУРИБ определяет категории потенциального ущерба (финансовый, репутационный, регуляторный, клиентский) от реализации каждого риска ИБ из области оценки. Далее определяется шкала уровня влияния (воздействия) каждого риска в зависимости от определенного ранее периода простоя бизнес-процесса для каждой категории ущерба. КУРИБ

также определяет шкалу вероятности реализации каждого риска (от 1 до 3 или от 1 до 5).

Анализ рисков ИБ проводится для определения уровней идентифицированных рисков с учетом вероятности их реализации и уровня потенциального воздействия на бизнес-процессы компании.

Для каждого риска члены КУРИБ оценивают уровень его влияния по каждой из категорий ущерба (финансовый, репутационный, регуляторный, клиентский). Уровень влияния документируется менеджером рисков.

Если в ходе оценки члены КУРИБ определили различные уровни ущерба для одного и того же риска, должен быть принят наихудший сценарий и в реестре зафиксирована самая высокая оценка.

Затем оценивается вероятность возникновения риска, и числовой эквивалент оценки вероятности заносится менеджером рисков в поле «Вероятность возникновения» реестра. И наконец, индивидуальная оценка риска для каждой категории ущерба определяется по формуле:

$$\text{Уровень риска} = \text{Вероятность} \times \text{Уровень влияния}$$

Вышеперечисленные характеристики рисков ИБ определяются путем мозгового штурма и НАЗОР.

На основании полученных данных путем усреднения индивидуальных уровней риска по категориям ущерба и последующего умножения на коэффициент критичности бизнес-процесса определяется интегральный уровень каждого риска ИБ :

$$\text{Интегральный уровень риска} = \frac{(Рфин + Ррег + Ррен + Ркл)}{4} \times \text{Коэффициент критичности,}$$

где $Рфин$ – уровень риска финансового ущерба;

$Ррег$ – уровень риска регуляторного ущерба;

$Ррен$ – уровень риска репутационного ущерба;

$Ркл$ – уровень риска клиентского ущерба.

Дальнейшие действия

Теперь нужно оценить возможность принятия каждого риска, т.е. сравнить интегральный уровень этого риска с критериями его принятия. Можно предложить следующие статусы принятия риска:

1. Не может быть принят. Уровень риска слишком высок, требуются немедленные действия с целью его снижения, например:

- разработать и применить соответствующие меры контроля;
- избегать риска с помощью корректировки или прекращения вызывающей его деятельности;
- передать риск другой стороне (страхование, аутсорсинг).

2. Может быть принят с дополнительными условиями. Риск признается допустимым, но, например, ввиду значимости бизнес-процесса требуется регулярный мониторинг для контроля его нахождения в допустимых пределах.

3. Может быть принят. Риск находится в допустимых пределах, немедленные действия не требуются. Рекомендуется осуществлять периодический мониторинг.

Одна из нетривиальных задач – определение варианта обработки каждого риска ИБ (способа воздействия на риск) на основании следующих типов воздействия:

- минимизация риска применением соответствующих мер контроля – усиление технических мер безопасности, обучение сотрудников и т.д.;
- избегание (исключение) риска: пересмотр или прекращение действий, способствующих возникновению риска;
- принятие или увеличение риска с целью его трансформации в возможность;
- устранение источника риска;
- изменение вероятности возникновения риска;
- изменение последствий реализации риска;
- обоснованное решение о сохранении риска;
- передача риска третьим сторонам (страховщикам, поставщикам и т.п.).

Вариант обработки риска ИБ выбирается исходя из экономической целесообразности, когда ресурсы, затрачиваемые на обработку риска, не превышают уровень воздействия его реализации на бизнес-процессы компании.



Анализ рисков непростая задача. И должен он проводиться параллельно с повышением уровня информационной безопасности компании. Если нет возможности выделить для этой работы специальное должностное лицо, как минимум менеджера рисков, то проще привлечь специалистов с рынка.

Если руководство компании понимает, что риски есть, их обязательно надо оценить. Хотя многие имеют большой «аппетит» к рискам и ждут, когда инцидент произойдет и нужно будет уже оценивать потери.



Полный текст статьи
читайте на
www.iksmedia.ru

[перечень публикаций 2024]

КОЛОНКА РЕДАКТОРА / № 1–4



- Когда их становится слишком много № 1
Производители реальные и виртуальные . . . № 2
Выставка достижений цдостроения. № 3
ИИ как цифровой МММ? № 4



ИКС-ПАНОРАМА / № 1–4



- Деньги, оборудование, ЦОДы № 1
Шестилетка цифровизации № 1
Российские облака: курс на экосистемы . № 2
Д. Хлебородов. Cloud X: каким должно быть ПО для облаков № 2
СКС: отказ от принципов как способ повышения коммерческой привлекательности № 2
К. Степанов. ЦОДы требуют специальной экспертизы. № 2



- Российские ЦОДы:
в тренде – комплексность № 3
Самый большой в Сибири № 3
ЦОДы прирастают Сибирью № 3
ЦОДы Санкт-Петербурга:
в ожидании роста № 3
ЦОД-2024. Время надежных № 4
Вслед за инновациями № 4
ДАЙДЖЕСТ ОТРАСЛИ ЦОДов № 1–4

ЭКОНОМИКА И БИЗНЕС / № 1–4



- Н. Носов. Страсти по ИИ, или Взлом операционной системы человеческой цивилизации № 1
А. Волков. Экспертиза и сервис – новые грани конкуренции на рынке ИБП № 1
Н. Носов. Блокчейн: жизнь после хайпа. . № 1
С. Вышемирский. От ветряных мельниц до атомных станций, или Насколько «зелеными» могут стать ЦОДы № 1
В. Хлебников. Лидерская позиция – это вызов, и мы его принимаем. № 1
Н. Носов. ЦОДы будущего: между искусственным интеллектом и «зеленой повесткой» № 2
И. Адякова. ДКС: наша задача – опережать рынок № 2



- Д. Доннеллан, Э. Лоуренс, Д. Бизо, М. Смолакс, Ж. Дэвис, Дж. О'Брайен. ЦОД-прогнозы 2024 № 2
И. Каменский. iTeaQ в России:
за комплексный подход № 2
Н. Носов. Как обеспечить доверие к российским ИТ: три стратегии № 3
Р. Шмаков. Ставка на экосистему № 3
Д. Доннеллан, Э. Лоуренс, Д. Бизо, М. Смолакс, Ж. Дэвис, Дж. О'Брайен. ЦОД-прогнозы 2024. Окончание № 3
А. Панин. Alcon DC Nord – технопарк и ЦОД премиальной надежности на Соколе № 3
Е. Вирцер. Всё в наших руках!. № 4
Н. Носов. Легализация майнинга в России: первый шаг сделан № 4

ИНФРАСТРУКТУРА / № 1–4



- А. Барков. ЦОДы для искусственного интеллекта № 1
Д. Хлебородов. Cloud X: какими должны быть облака № 1
Э. Лоуренс, Л. Саймон. Анализ отказов в ЦОДах. Окончание. № 1
Т. Чирков, К. Нагорный, А. Чеснов. Служба эксплуатации ЦОД. Глава из книги № 1
Н. Носов. Импортозамещение сетевого оборудования: успехи и пробелы № 1
А. Семенов. Исчерпала ли себя многомодовая оптика в ЦОДе? № 1



- Е. Оганесян. За что платим? Споры о длине витой пары в СКС и как их избежать . . . № 1
А. Семенов. Про СКС по-русски. № 2
А. Пахомов. СКС для ЦОДов, или Что объединяет смородину, вяз, багрянник и можжевельник? № 2
А. Барков. Сервис ИБП. Чего хотят заказчики № 2
Д. Шпанько. От ИБП к комплексным решениям № 2
М. Смолакс. Повторное использование тепла ЦОДов № 2

- Литий-ионные батареи для ИБП:
стоит серьезно задуматься. № 2
- Т. Чирков, К. Нагорный, А. Чеснов. Служба
эксплуатации ЦОД. Глава из книги.
Окончание. № 2
- Третье поколение шкафов
ПРОЦОД DS V3 от NTSS: еще лучше,
еще удобнее № 2
- А. Барсков. Надежность систем ИБП.**
Что выбирают ЦОДы № 3
- В. Сильвестрова. Итальянское качество
при стабильных поставках. № 3
- Д. Шпанько. Когда ЦОДы становятся
большими № 3
- А. Мартынук. Экономика проекта
выходит на первое место. № 3
- Ю. Барабанчиков. ЦОД на российских
решениях. Опыт интегратора № 3
- А. Сараев. NED на рынке инноваций
для ЦОДов. № 3
- Г. Дрягин. Среда общих данных
как основа BIM/TIM № 3
- Е. Кривоносов, С. Довгань.
Еще раз про DCIM № 3
- Н. Носов. Виртуализация сети:
от VLAN до VPN. № 3
- С. Хуторной. EKF – новый игрок
на рынке телеком-оборудования
для ЦОДов. № 3
- М. Саликов. Энергоцентры высокой
плотности для ЦОДов. № 3



- Е. Оганесян. Калибровка, поверка
и точность сертификационных
измерений в СКС № 3
- Д. Белоусов. Чиллеры Dunham-Bush
для российских ЦОДов № 3
- А. Барсков. Моновендорный ЦОД**
или комплексный подход № 4
- ДКС: если предлагать,
то производить самим № 4
- Н. Носов. Виртуализация сетей:
время облаков № 4
- Н. Носов. ЦОД-2024. Инфраструктура
для облака № 4
- С. Вышемирский. ЦОД для ИИ.
IXcelerate уже строит № 4
- Н. Носов. Специфика сетей
для искусственного интеллекта. № 4
- И. Бедердинов. Серверы для ИИ:
что предлагают российские
производители. № 4
- В. Новиков. Итальянские системы
охлаждения в России: профессионализм
и стабильность № 4
- Е. Шлык. ДГУ в России: поиски пути . . . № 4
- А. Беспалов. От аккумуляторов
до стоек и PDU мирового уровня. № 4
- К. Хэслер. Чем тушить ЦОДы № 4
- А. Семенов. Есть ли будущее
у многопарных LAN-кабелей?. № 4
- EMILINK: в стремлении к технологическому
суворинству и лидерству в ЦОДах . . . № 4



- Н. Носов. Облачные библиотеки**
и российский рынок DBaaS № 1
- Н. Носов. Облако-суперкомпьютер . . . № 1
- О. Роджерс. Там, где облако встречается
с периферией. № 1
- Н. Носов. Российское ПО виртуализации.**
Новые вызовы и предложения № 2
- Российский интернет вещей из облака . . № 2
- А. Салов. Облачные итоги-2023.
Глобальный рынок. № 2



СЕРВИСЫ И ПРИЛОЖЕНИЯ / № 1-4

- Н. Носов. Прыжок в эру ИИ, или
Пять вопросов к проекту «Экономика
данных» № 3
- О. Федоров. Пять принципов
бесперебойной работы
ИТ-инфраструктуры. № 3
- А. Кузнецова. Коммерческий open
source: за и против № 4
- Н. Маркашов. Мобильные приложения
под санкциями № 4

- Н. Носов. Информационная**
безопасность: турбулентный 2023. . . . № 1
- Н. Носов. Регулирование ИБ:
защищать и развивать № 1
- Н. Носов. Кибербезопасность-2024.**
Основные тренды № 2
- Н. Носов. ЦОД как узел защиты
от квантовых угроз № 2



БЕЗОПАСНОСТЬ / № 1-4

- Н. Носов. Не по правилам № 3
- Н. Носов. ЦОДы и кибербезопасность. . № 3
- Н. Носов. Российские MSSP: рынок**
и тенденции. № 4
- Н. Носов. Искусственный интеллект
и угрозы информационной
безопасности № 4
- НОВЫЕ ПРОДУКТЫ. № 1-4



ДИ СИ КВАДРАТ Тел.: (800) 600-9212 E-mail: info@dcxdc.ru https://dcxdc.ru/.....1-я обл., с. 16-19	ЦИФРОВОЙ ОСТРОВ Тел.: (985) 088-0885 E-mail: tn@d-ostrov.ru https://d-ostrov.ru/.....с. 22-23	ENVICOOL https://ru.envicool.com/.....с. 52-53
ПАРУС ЭЛЕКТРО Тел.: (495) 518-9292 E-mail: info@parus-electro.ru https://parus-electro.ru/.....с. 4-5	ABSolute Тел: (495) 103-1412 E-mail: info@ab-solution.ru https://ab-solution.ru/с. 40-41	IPPON Тел: (499) 226-2634 www.ippon.ru.....с. 46-47
СВОБОДНЫЕ ТЕХНОЛОГИИ ИНЖИНИРИНГ Тел.: (495) 120-2866 E-mail: info@sv-tech.ru www.sv-tech.ruс. 11	ALCON GROUP Тел.: (495) 967-6923 E-mail: info@alcongroup.ru https://alcongroup.ru/с. 29	KEY POINT Тел.: (495) 120-2866 E-mail: info@keypoint-group.ru https://keypoint-group.ru/4-я обл.
		VSP GLOBAL Тел: (499) 499-1952 E-mail: info@vspglobal.ru www.vspglobal.ruс. 30-31

Указатель фирм и организаций

3data	50	K2 Cloud	62	«Базис»	56, 57, 58, 59	МТУСИ	25
451 Research	48	ГК Key Point	6, 7, 8, 9	ИЦ «Баррикады»	58	«Неорганические	
Ackermann	26	Larsen & Toubro	10	БСС	58	сorbенты»	32
AT&T	67	M1Cloud	66	ВК	57, 58	НИУ ВШЭ	20
Avanpost	72	Materion Corporation	74	Всемирная ядерная		«Нума Технологии»	58
AWS	66	McKinsey	13, 21	ассоциация	9	«Онлант»	60, 64
Axoft	72	Microsoft	42	ВТБ	58	«Орион софт»	55, 56,
Beeline Cloud	61	Mordor Intelligence	21,	«Гиперлайн»	25	57, 58, 59
Bluemix	67	69, 73	«Гостех»	57	«Парус электро»	4, 5
Broadcom	55, 67	MTS Web Services	10, 62	«ДАКОМ М»	58, 59, 60	ГК «Пожтехника»	51
Cloud.ru	66	Net One	10	Департамент энергетики		«Рег.ру»	64
Cloud X	59	Nvidia	1, 58	США	44	РЕД СОФТ	57, 58
Cray	42	OVHcloud	48, 49	«Ди Си квадрат»	7, 16	«Рокитсофт»	58
DataLine	49	Oxygen.	63	«ДиСиСи»	32	НТЦ ИТ РОСА	55, 57, 58
DataSpace.	50	Qtech.	38, 39	«ИКС-Медиа»	6, 8, 9, 56	«Росатом»	6
DataVolt	9, 10	RCCPA	65	ГК «Инновационные системы		«Росплатформа»	58
East Telecom	9	Red Hat	57, 58	пожаробезопасности»	50	Россельхозбанк	56
EDGEЦентр	66	Selectel	58, 63, 66, 67	Институт программных		Росстат	69, 72
Eltex	38, 39	Servers.ru	66, 67	систем им. А.К. Айла-		«Ростелеком»	57
Eni S.p.A.	42	Softlayer	67	мазяна РАН	43, 45	«Р-ПЛАТФОРМА»	58
Envicool	52	ГК Softline	10, 20	«Инфосистемы Джет»	55	«РСХБ-Интех»	56
Exepto.ru	67	Softline Digital	20	ИСИЭЗ НИУ ВШЭ	21	ГК «РТК-ЦОД»	6, 7, 10, 66
Expert Market Research	73	Statista.	13	«ИСПсистем»	58	«РусБИТех-Астра»	58
Fozzy.ru	67	Strategy Partners	73	«ИТГЛОБАЛКОМ		РФЯЦ-ВНИИЭФ	44
Gartner.	13	Synergy Research Group	7	Лабс»	56, 58	Сбербанк	43, 57
Global Insight Services	61	TAdviser	66, 73	«ИЭК Холдинг»	74	«Селектел»	58
GPUdс	61	Uptime Institute	7, 32,	«К2 Интеграция»	58	«Ситроникс»	58
GreenMDC.	10	33, 48, 51	«Киберпротект»	58	«Ситэкс»	32
Hewlett Packard Enterprise	42	Vertiv	1	«Ключевые ИТ решения»	58	«Т-Платформы»	43
HPC Park.	62	VK Cloud.	66	«КонсалтингПроф»	58	УЦСБ	7
HPE.	42	VK Tech	66	АНО «Координационный		«Холдинг ОСК групп»	50
Huawei	1, 57	VMware	55, 62, 67	совет по ЦОДам и облачным		ИК «ХОСТ»	57, 58
IBM	67	VSP Global	30, 31	технологиям»	10	ЦБ РФ	73
IBM Cloud	67	vStack	56, 58	КРОК.	58	Центр организации	
iKS-Consulting	6, 7, 56, 57, 59, 65, 66, 67, 69, 73	YADRO	38, 39	«Лаборатория		дорожного движения	23
immers.cloud	62	Yandex Cloud	66	Касперского»	72, 73	«Центр стратегических	
Ippon.	46, 47	«Абсолютные Решения»	40	ГК ЛАНИТ	60	разработок»	70, 71,
ITglobal.com.	62	«Аквариус»	38	НИИ «Масштаб»	58	72, 73
ITPOD	37	ГК «Астра»	56, 57, 58, 59, 60	МГУ им. М.В. Ломоно-		«Цифровой остров»	22, 23
IXcellerate	13, 51	«Аэродиск»	58	сова	43	«Шаркс Датацентр»	58
		ГК Б1.	72	Минпромторг.	38, 39	Шереметьево	56
		«Базальт СПО»	58	Минэнерго России	32, 35	Юлихский супер-	
				МТС	10, 42	компьютерный центр	45
						«Яков и партнеры»	20
						«Яндекс»	42, 50, 51, 66

Учредитель журнала «ИнформКурьер-Связь»:

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

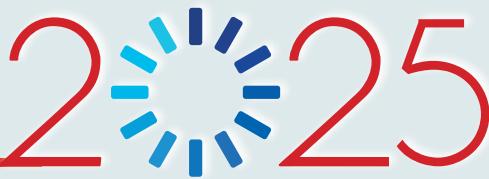


12-й ЕЖЕГОДНЫЙ ФОРУМ

DATA CENTER DESIGN & ENGINEERING

20 мая

Москва, Holiday Inn Moscow Sokolniki



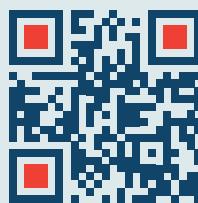
Серьезные изменения состава игроков на рынке инженерных систем ЦОДов происходят на фоне трансформации требований к таким системам. Рост числа и масштабов ЦОДов, проблемы с доступностью энергетических ресурсов, повышение спроса на высоконагруженные стойки, развитие альтернативных систем охлаждения – для грамотной реакции на все это необходим оперативный обмен технической информацией, наилучшим опытом и практиками проектирования, построения и эксплуатации ЦОДов.

Фокус DCDE-2025

- Инженерная инфраструктура для ИИ: эволюция или революция
- Где взять энергию для ЦОДов: перспективы локальной генерации
- Новые технологии аккумулирования электроэнергии
- Готовы ли системы прямого жидкостного охлаждения к массовому использованию в ЦОДах
- Адаптивная инфраструктура на вырост: закапывание денег или разумные инвестиции



подробно о программе и участниках
на сайте форума dcdeforum.ru





РЕГИОНАЛЬНАЯ СЕТЬ ЦОД ГРУППЫ КОМПАНИЙ KEY POINT ВАЖЕН КАЖДЫЙ!



ДАТА-ЦЕНТРЫ С СЕРТИФИКАЦИЕЙ TIER III



Реклама

keypoint-group.ru