ТЕМА НОМЕРА

СТРАСТИ ПО ИИ

ИнформКурьер-Связь
ИКС
издается с 1992 года

Systême electric

Энергия. Технологии. Надежность.

Мы — российская компания с мировой экспертизой, производим и поставляем оборудование и комплексные решения для проектов по передаче и распределению электроэнергии и автоматизации. **Systeme Electric** предлагает клиентам и партнерам единую экосистему продуктов и решений SystemeOne на базе российского программного обеспечения.

3000+
сотрудников

Крупнейший в отрасли инженерно-сервисный центр (г. Москва)

Завод «Потенциал»
(г. Козьмодемьянск)

Механотроника
НТЦ «Механотроника»
(г. Санкт-Петербург)

18
офисов в России и Беларуси

2
логистических центра

Завод «СЭЗЭМ»
«Систэм Электрик Завод Электро-Моноблок» (г. Коммунар)

Systême soft
Центр инноваций Systeme Soft
(г. Иннополис)

ПРИГЛАШАЕМ НА КЛЮЧЕВОЕ СОБЫТИЕ В СФЕРЕ ЭЛЕКТРОЭНЕРГЕТИКИ И АВТОМАТИЗАЦИИ

ИННОВАЦИОННЫЙ САММИТ 2024

Технологическое партнерство — объединяем лучшее

РЕГИСТРИРУЙТЕСЬ СЕЙЧАС!

15-18 апреля 2024
Москва, ЦВК «Экспоцентр», павильон 3

systeme.ru

Реклама / 16+

Издается с мая 1992 г.

Издатель
ООО «ИКС-МЕДИА»

участник
АНО КС ЦОД
КООРДИНАЦИОННЫЙ СОВЕТ ПО ЦОДам И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ
Автономная некоммерческая организация

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

Учредитель:
ООО «ИКС-МЕДИА»

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

РЕДАКЦИЯ
iks@iksmedia.ru

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

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

Корректор
Е.А. Краснушкина

Дизайн и верстка
Е.В. Денисова

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

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

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

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

Дата подписания в печать: 01.03.24.
Дата выхода в свет: 12.03.24.
Тираж 5 000 экз. Свободная цена.
Формат 64x84/8
Типография: ООО "ПРОПЕЧАТЬ",
адрес типографии 119618, г. Москва,
Боровское ш., дом 2А, корп. 4, кв. 260.

ISSN 0869-7973

Когда их становится слишком много

Сколько операционных систем мы знали раньше? Windows, Linux, MacOS... – можно сосчитать по пальцам одной руки. А сейчас? Захожу в Единый реестр российских программ для ЭВМ и баз данных. Задаю класс «операционные системы общего назначения». Результат – 41 ОС. Сорок одна! А еще восемь мобильных ОС, да 10 операционных систем реального времени. Итого – почти 60 (и это только по новому классификатору, утвержденному в сентябре 2020 г.). Похожая ситуация и с системами виртуализации: в реестре их десятки. А раньше опять же можно было сосчитать на пальцах: VMware, Hyper-V, KVM, Xen.

Хорошо это или плохо? Для развития отечественной индустрии программного обеспечения в этом, возможно, есть свои плюсы. Но на что ориентироваться заказчикам? Им проще, когда есть три–пять проверенных продуктов с доказанными характеристиками, надежностью и безопасностью. И к этому рынок ПО обязательно придет.

Посмотрим на ситуацию с аппаратным обеспечением. Возьмем, для примера, мощные трехфазные ИБП – необходимый элемент для ЦОДов, в которых сейчас «крутится» большинство прикладных систем. Число производителей таких систем на российском рынке тоже сильно выросло. Как точно заметил один из экспертов, каждый реселлер норовит выйти в «производители», завозя китайские ИБП и без стеснения заявляя, что они отечественного производства. Конечно, и в этом сегменте количество предложений со временем уменьшится. Останутся те, кто сможет доказать качество продукции, обеспечить адекватную экспертизу и сервис.

Но для тех же ИБП ситуация с реестром принципиально иная. По понятным причинам с «железом» попасть в реестр гораздо сложнее, чем с софтом. И в данном случае речь о Едином реестре российской радиоэлектронной продукции, который ведет Минпромторг. Мощные трехфазные ИБП в нем присутствуют лишь от одного российского производителя (рекламу делать не буду – посмотрите сами).

«ИКС» старается помочь заказчикам разобраться в свалившемся на них разнообразии. Мы каждый год готовим «Карту вендоров» по основному инженерному оборудованию для ЦОДов. По программным продуктам выпускаем «Карту ПО виртуализации», очередной релиз которой выйдет к конференции Cloud & Connectivity (она состоится 21 марта). Сами конференции – хорошая возможность ближе познакомиться с продуктами, в живом общении оценить экспертизу их поставщиков, договориться о тестировании. И выбрать оптимальный вариант.

До встречи на наших конференциях,
Александр Барсков

Страсти по ИИ, или Взлом операционной системы человеческой цивилизации → с.14

Шестилетка цифровизации

с. 23

С. Вышемирский. Насколько «зелеными» могут стать ЦОДы

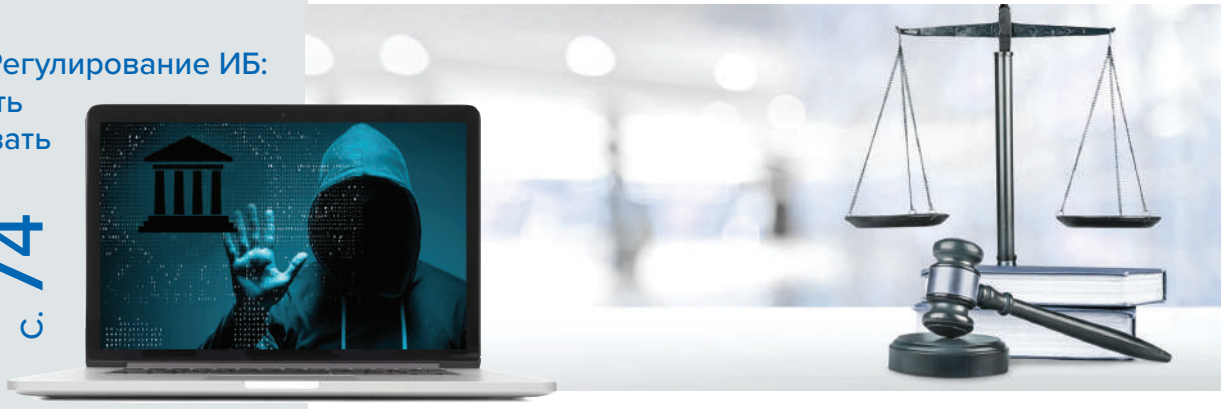

с. 44

Н. Носов.
Импортозамещение сетевого оборудования: успехи и пробелы


с. 63

Н. Носов.
Облако-суперкомпьютер

Н. Носов. Регулирование ИБ: защищать и развивать


с. 74

ЦОД Екатеринбург DATA CENTER FORUM

Деньги, оборудование, ЦОДы

Благодаря новым проектам на Урале, как и в большинстве регионов России, растет количество стойко-мест в коммерческих ЦОДах. У этих объектов явно определен уровень готовности, что гарантирует надежную работу ИТ-систем.

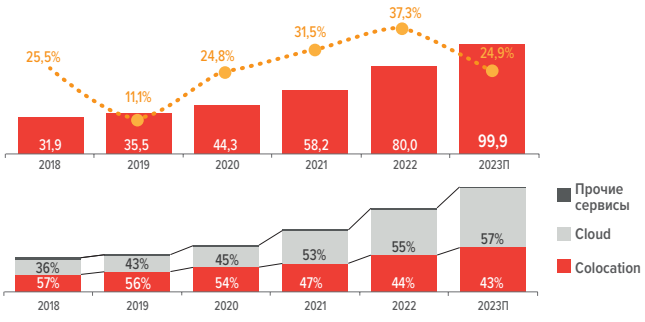
Конференция «ЦОД: модели, сервисы, инфраструктура» в Екатеринбурге, которую «ИКС-Медиа» провела уже в пятый раз, интересна тем, что на ней помимо обсуждения региональных проектов подводятся предварительные итоги года в российской отрасли ЦОДов. В нынешнем году для более чем 300 делегатов актуальным оказался и обмен опытом применения технических решений новых вендоров.

В 2023 г. количество стойко-мест в коммерческих ЦОДах в России, по данным iKS-Consulting, увеличилось почти на 21% (рис. 1), что вдвое больше показателя предыдущего года. Согласно позитивному сценарию развития, такой рост продолжится и в следующем году, а в 2025–2026 гг. средний рост составит 18%. Этот сценарий предполагает, что спрос на уровне 12–14 тыс. стойко-мест в год сохранится. Есть и более консервативный сценарий, в соответствии с которым после ввода в эксплуатацию большого числа стойко-мест в 2023–2024 гг. возникнет профицит предложения и спрос снизится. В этом случае средний показатель роста в 2025–2026 гг. достигнет лишь 12%. Но аналитики iKS-Consulting больше ориентируются на позитивный сценарий.

В денежном выражении рынок коммерческих ЦОДов в 2023 г. вырастет еще больше – примерно на 25%. Однако это существенно ниже прироста в 2022 г. – 37,3% (рис. 2). Доля облачных сервисов стабильно увеличивается (57% в 2023 г. против 55% годом ранее), а услуг colocation снижается (43% в 2023 г. против 44% в 2022-м). В сегменте облаков наибольший рост показывают инфраструктурные сервисы: PaaS – 37%, IaaS – 30%.

Источник: iKS-Consulting

▲ **Рис. 1. Динамика рынка коммерческих ЦОДов в России, стойко-мест**



Источник: iKS-Consulting

▲ **Рис. 2. Динамика рынка коммерческих ЦОДов в России, млрд руб.**

Сооснователи ГК Key Point Евгений Вирцер (слева) и Александр Мартынюк на церемонии закладки первого камня ЦОДа в Свердловской области

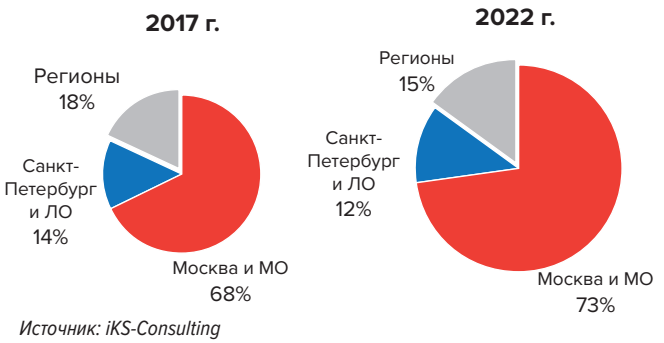
Первый камень и будущий ЦОД Key Point

Что касается территориального распределения мощностей коммерческих ЦОДов, то три четверти таких объектов сосредоточены в Москве. И доля столицы растет: с 68% в 2017 г. до 73% в 2022 г. (рис. 3). Главная причина этого, по мнению Станислава Мирина, ведущего консультанта iKS-Consulting, в том, что подавляющее большинство управляющих офисов компаний из топ-500 расположено в Москве. Приход в коммерческие ЦОДы компаний с более равномерным размещением бизнеса по стране может увеличить долю региональных ЦОДов.

Даешь 2000 стоек!

Сегодня в России не так много компаний активно строят коммерческие ЦОДы в регионах. К лидерам этого направления можно отнести Key Point и «Ростелеком-ЦОД». Первая в июне 2022 г. анонсировала строительство 35 дата-центров в течение ближайших шести-семи лет во всех федеральных округах РФ. В феврале 2023 г. ГК Key Point запустила в эксплуатацию первую очередь ЦОДа во Владивостоке (на 440 стоек) и сейчас строит вторую очередь такой же емкости. 30 января 2024 г. компания ввела в эксплуатацию первую очередь аналогичного по емкости ЦОДа в Новосибирске. А 29 ноября 2023 г. был заложен первый камень ЦОДа на 880 стоек, который будет построен в индустриальном парке Craft под Екатеринбургом.

Говоря о предпосылках создания ЦОДов в регионах, Александр Мартынюк, сооснователь ГК Key Point, указывает на высокую загрузку магистральных каналов связи и ограниченные возможности их расширения.



Источник: iKS-Consulting

▲ **Рис. 3. Доли регионов на рынке коммерческих ЦОДов в России**

И то и другое повышает привлекательность локального хранения и обработки больших объемов данных – не нужно тратить огромные средства на их передачу в центр. Кроме того, он отмечает высокий спрос со стороны федеральных и локальных облачных компаний, работающих с местным бизнесом, а также потребность технологичных компаний в качественной локальной инфраструктуре.

Важными особенностями проектов Key Point А. Мартынюк называет модульный подход, который позволяет масштабировать и наращивать емкости ЦОДов в соответствии со спросом, и однотипность решений, что дает возможность создать единую службу эксплуатации, добиться максимально комфортных условий у производителей основного оборудования, сэкономить время на проектно-изыскательных и строительно-монтажных работах и предоставить клиентам один и тот же уровень SLA вне зависимости от местонахождения объекта. Все ЦОДы обязательно сертифицируются по уровню отказоустойчивости Tier III (это удовлетворяет технологическим требованиям 99,5% клиентов). А независимость объектов от операторов связи и присутствие в них нескольких операторов повышают привлекательность ЦОДов для клиентов и расширяют их круг.

Проект создания ЦОДа под Екатеринбургом, как рассказал Евгений Вирцер, сооснователь ГК Key Point, подобно другим проектам компании, будет реализован в два этапа. Первый этап предусматривает строительство административно-бытового корпуса и технологической части ЦОДа вместимостью 330 ИТ-стоек мощностью по 7 кВт. На втором этапе будет возведена технологическая часть дата-центра емкостью 550 ИТ-стоек. Запуск в эксплуатацию первой очереди намечен на 1 октября 2024 г. «Спрос чувствуем. Не исключено, что вторую очередь начнем оснащать, еще не закончив первую», – отметил Е. Вирцер.

В числе технологических особенностей нового ЦОДа Key Point – использование энергоблоков заводского изготовления (это готовые изделия, предназначенные для бесперебойного электроснабжения критических систем дата-центра) и систем естественного охлаждения. Объект будет иметь уникальную архитектуру, поддерживающую статус Екатеринбурга как исторической столицы конструктивизма. В стадии проработки сейчас находятся ЦОДы в

Слева направо: Дмитрий Горкавенко (iKS-Consulting), Алексей Соловьев (Systeme Electric), Алексей Солодовников (Uptime Institute), Дмитрий Бедердинов (АНО КС ЦОД), Евгений Вирцер (Key Point)

Ставрополе (это будет самый большой коммерческий ЦОД в ЮФО с подведенной мощностью 16 МВт), Южно-Сахалинске, Архангельске и Махачкале.

Георазпределенная сеть дата-центров компании «Ростелеком-ЦОД» уже насчитывает 21 узел (20,5 тыс. стоек), в том числе в Удомле (Тверская область), Новосибирске и Екатеринбурге (рис. 4). Первая очередь ЦОДа «Екатеринбург» была введена в эксплуатацию в ноябре 2019 г. В ноябре 2023 г. компания закончила комплексные испытания основного технологического оборудования второй очереди, ввод которой в эксплуатацию увеличит число стойко-мест до 430 (потребляемая мощность – 4 МВт).

К трудностям текущего этапа цодостроительства (с которыми «Ростелеком-ЦОД» столкнулся при реализации второй очереди ЦОДа «Екатеринбург») Денис Тарасов, директор обособленного подразделения компании, отнес то, что новые азиатские производители зачастую не учитывают особенности, указанные заказчиком в ТЗ, а отечественные производители берутся за изготовление и поставку оборудования, не имея достаточного опыта, что приводит к многократным доработкам изделий. Вместе с тем есть и положительные моменты: производители с легкостью идут на изменения и доработку оборудования на строительной площадке без потери гарантии.

«В треугольнике “сроки – цена – качество” мы решили сохранить цену и качество в ущерб срокам. Сократили транспортные расходы, выбрав местных производителей строительных материалов. Благодаря ценовой политике новых поставщиков, несмотря на рост цен на стройматериалы и повышение материалоемкости объекта, мы остались в рамках бюджета», – подчеркнул Д. Тарасов. Также он отметил, что компания изменила подход к пусконаладке: раньше проводили тестирование только на этапе комплексных испытаний (учитывая опыт построения ЦОДов на оборудовании известных брендов), теперь же нагрузочное тестирование на номинал проводится для каждой подсистемы.

В планах развития ЦОДа «Ростелеком-ЦОД» в Екатеринбурге предусмотрены реализация третьей (214 стоек) и четвертой (800 стоек) очередей. Даже если полагаться на планы только двух упомянутых компаний, общая емкость коммерческих ЦОДов в столице Урала превысит 2 тыс. стоек.

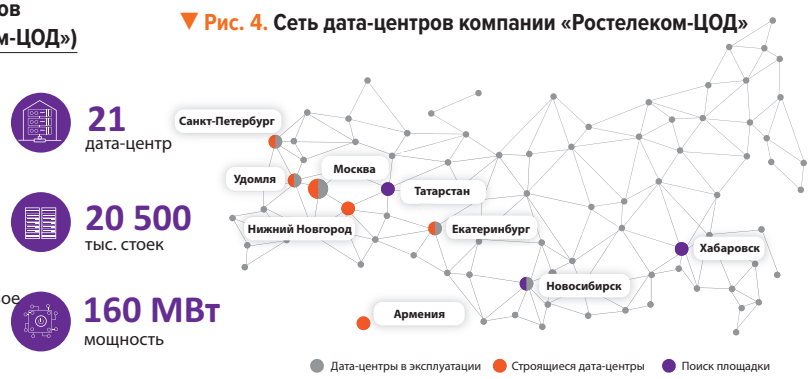
Где брать деньги

Сегодня создание ЦОДов серьезно сдерживают высокая стоимость капитала и связанное с этим увеличение сроков окупаемости инвестиций. Но цодостроители духом не падают.

«У нас два источника финансирования – инвесторы и банки. За последние два года банки стали поворачиваться лицом к цодовским проектам. По крайней мере пятьшесть банков (из первой тридцатки) понимают, что такое ЦОДы, готовы идти в эти проекты и при определенных условиях с удовольствием их финансируют, – делится опытом Е. Вирцер. – Конечно, велики валютные

Денис Тарасов («Ростелеком-ЦОД»)

▼ Рис. 4. Сеть дата-центров компании «Ростелеком-ЦОД»



риски, которые трудно прогнозировать. В этом плане сложным оказался наш новосибирский проект. Начинали мы при курсе доллара 60–65, а основные расходы пришлось делать при курсе 90–100. Отчасти помогла оптимизация технических решений. И хотя построили дороже, чем планировали, запас по окупаемости позволяет считать этот проект успешным».

«В рамках программы «Экономика данных» мы сделали ряд предложений по поддержке ЦОДов, – рассказывает генеральный директор АНО «Координационный центр по ЦОДам и облачным технологиям» Дмитрий Бедердинов. – Ключевое – это льготное кредитование строительства новых объектов. При увеличившихся процентных ставках по кредитам и росте цен на оборудование компании испытывают трудности в привлечении средств на запуск новых проектов, поскольку в сегодняшних условиях срок окупаемости составляет 15 лет и выше. Льготное кредитование предполагает, что операторы дата-центров смогут получать кредиты не более чем под 5% годовых (сейчас ставка доходит до 20%)». Это поможет операторам развивать цифровую инфраструктуру, что особенно важно для региональных проектов.

В Москве волна строительства новых ЦОДов во многом связана с выходом на этот рынок девелоперов. «Они профессионально подбирают площадки, эффективно взаимодействуют с энергетиками и умеют привлекать финансирование, – указывает Алексей Солодовников, управляющий директор Uptime Institute по России и СНГ. – И я не вижу причин, почему бы эту практику не продолжить в Екатеринбурге, равно как и в других регионах».

Алексей Соловьев, технический директор управления по рынку «ИТ-решения» компании Systeme Electric, напоминает о роли вендоров в привлечении инвестиций. По его мнению, проект ЦОДа с известным вендором, берущим на себя определенные обязательства, с понятными технологиями и предсказуемым развитием имеет большие шансы на получение финансирования. «И это относится не только к коммерческим ЦОДам. Мы часто помогаем продвигать проекты корпоративных ЦОДов внутри компаний», – добавляет он.

Важна и возможность снижения капитальных затрат. «Не затягивайте с принятием решения. Стоимость денег сегодня высока, поэтому оперативное принятие решения может дать существенную экономию. Если же медлить, то придется или увеличивать бюджет, или урезать функционал, – советует А. Соловьев. – Я за модульный подход. Он позволит не переразмеривать ЦОД на первом этапе и обеспечит возможность быстрого роста».

«Рекомендуем максимально использовать системы высокой заводской готовности, – говорит Е. Вирцер. – Переход на префабы дает возможность изготовить большую часть инфраструктуры в заводских условиях, серьезно повысить качество и сэкономить время. А время, как известно, это самый главный финансовый ресурс».

Где брать оборудование

Сегодня для реализации цодовских проектов по большому счету есть три источника оборудования. Это параллельный импорт (оборудования известных вендоров), новые производители из восточных стран и отечественные предприятия.

Источник: УЦСБ

▲ **Рис. 5. Источники оборудования для разных сценариев**

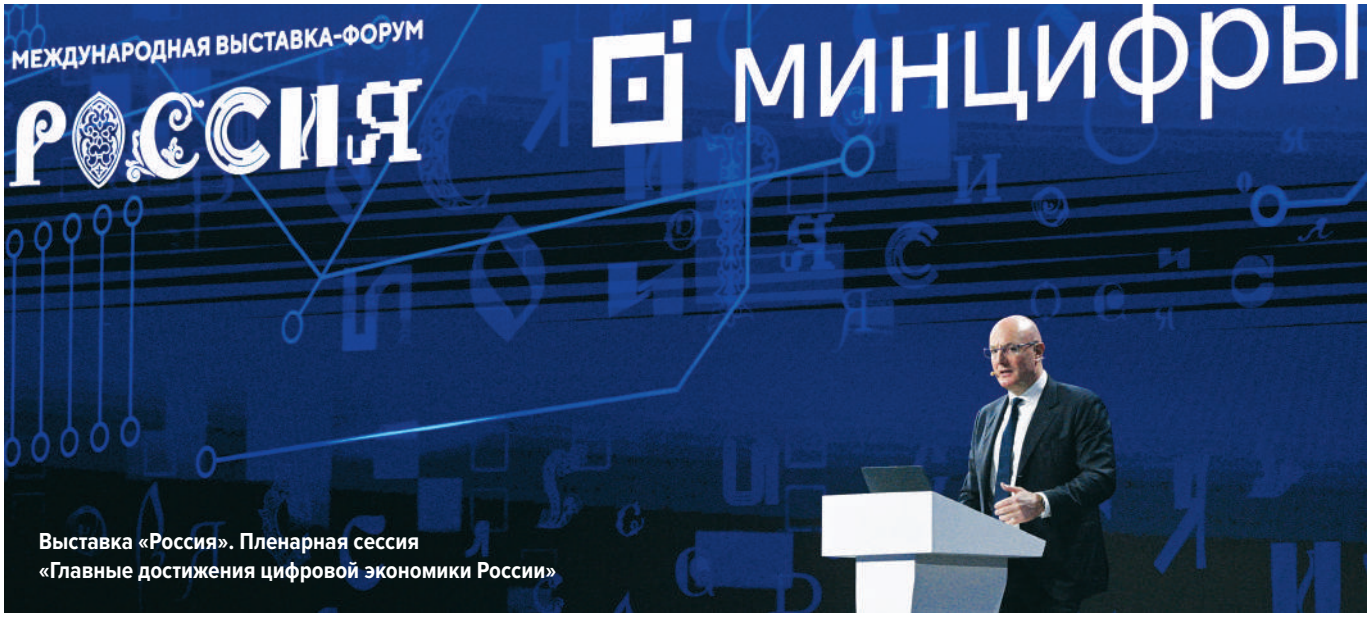
Несмотря на многочисленные риски параллельного импорта и высокую стоимость этого варианта, к нему все же приходится прибегать, например, когда необходимо дооснастить объект, особенности которого не допускают применения оборудования других вендоров. Однако в большей части сценариев предпочтение отдается новым вендорам (рис. 5).

Положительными моментами работы с новыми восточными производителями Олег Сидоров, заместитель директора технического департамента Уральского центра систем безопасности, называет доступность поставок и адекватную стоимость. Однако есть и риски: технические (касающиеся как самого решения, так и документации), организационные, санкционные, а также связанные с доступностью запчастей и сервиса. При работе с такими производителями эксперт УЦСБ считает важным прояснить вопросы представленности компании в России: наличие юридического лица, складов, компетенций и организации сервиса.

Что касается отечественных производителей, то к числу очевидных преимуществ работы с ними можно отнести доступность поставок (хотя сроки могут не выдерживаться), возможность глубокой кастомизации и короткое расстояние до производства. Однако нужно со вниманием относиться к степени локализации, доступности компонентной базы, мощности производства и, конечно, к организации сервиса.

В целом, как считает О. Сидоров, простых вариантов сегодня нет, а значит, тем большая ответственность ложится на плечи интеграторов, которые должны максимально изучить все возможности и риски. Собственно говоря, этот вывод относится ко всей отрасли ЦОДов: всем ее игрокам непросто, но это не отменяет развития на основе грамотного управления рисками и эффективного использования новых возможностей.

Александр Барсков
Екатеринбург – Москва



Выставка «Россия». Пленарная сессия «Главные достижения цифровой экономики России»

Фото: К. Зыков/фотохост-агентство РИА Новости

Шестилетка цифровизации

С принятия летом 2017 г. программы «Цифровая экономика Российской Федерации» минуло шесть с половиной лет. Проходящая на ВДНХ выставка-форум «Россия» дала повод подвести некоторые итоги. 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | 2023

Вызовы и изменения

Информационные технологии давно стали неотъемлемой частью жизни страны, и их роль продолжает расти. В частности, как сообщил на проведенном в рамках выставки-форума Дне цифровизации вице-премьер Дмитрий Чернышенко, в 2023 г. число пользователей портала Госуслуг по сравнению с 2019 г. увеличилось почти вдвое и достигло 109 млн человек. И если в 2019 г. цифровая зрелость ключевых отраслей экономики составляла 32%, то сегодня она превышает 74%. При этом уровень проникновения цифровых технологий в бизнес-процессы в 2023 г. вырос на 10,5% больше запланированного (рис. 1).

Начался переход к экономике данных – глобальной цифровой экосистеме, в которой данные рассматриваются как товар в сложных цепочках создания новой ценности (рис. 2).

Огромный импульс развитию ИТ дали пандемия COVID-19 и вызванный ею массовый переход на удаленную работу. Радикально изменил ИТ-ландшафт 2022 г. – санкции и уход с российского рынка зарубежных компаний подтолкнули процессы импортозамещения и способствовали росту российских ИТ-компаний.

Преобразившийся телеком

Существенно изменился телеком. Согласно исследованиям ИАА TelecomDaily, средняя скорость мобильного интернета в Москве за последние пять лет выросла в два раза: с 31 Мбит/с в 2019 г. до 63,2 Мбит/с в 2023 г. Рост в полтора-два раза наблюдался и в регионах.

Одним из основных драйверов развития телекома генеральный директор TelecomDaily Денис Кусков назвал документальную электросвязь (ДЭС, этот вид связи обеспечивает передачу сообщений, представленных в виде документов). По оценкам Росстата, объем рынка ДЭС вырос с 600,26 млрд руб. в 2018 г. до 795,453 млрд руб. в 2022-м (рис. 3).

Операторы связи в результате своих многолетних усилий не остаться только «трубой» для передачи голоса и данных вырастили целые экосистемы самых разных сервисов, включая облачные. Сформировались новые рынки: промышленный интернет вещей (IIoT), оказывающий огромное влияние на эффективность бизнеса по всем вертикалям; интернет вещей для физлиц (Consumer IoT), проникший практически во все сферы жизни – досуг, спорт, здоровье и даже на кухню. Уверенно растет рынок решений для «умного» дома (рис. 4). Мобильный интернет выступает драйвером развития мобильных экосистем, прежде всего мобильных приложений.

Сильное влияние на смежные рынки – ТВ и киноиндустрию – начали оказывать онлайн-кинотеатры. Например, президент «Ростелекома» Михаил Осеевский с гордостью сообщил, что у принадлежащего оператору онлайн-кинотеатра Wink 12,9 млн подписчиков, а представленный на этом ресурсе киносериал «Слово пацана. Кровь на асфальте» стал самым популярным в России даже до выхода на ТВ.

Еще один компонент экосистемы сервисов – услуги обеспечения кибербезопасности. Тот же «Ростелеком» приобрел с данной целью одного из лидеров рынка инфо-

беза компанию «Солар». К слову, диверсифицируя бизнес, наш телеком-гигант занялся импортозамещением оборудования ушедших с российского рынка вендоров: на подходе опытные образцы для новых базовых станций. Компания вкладывает средства и в разработку оборудования для спутниковой связи.

Своими экосистемами обзавелись и другие лидеры рынка телекоммуникаций. При этом они, меняя позиционирование на рынке, меняют и бренды, делая акцент на «цифре». «Ростелеком» отказался от напоминающего о голосовой связи «уха», «ЭР-Телеком Холдинг» («Дом.ру») рассматривает себя как «новый элемент цифровой экономики» и свой новый бренд ассоциирует с цифровыми стенами вокруг дома. Стремится закрепить за собой звание цифровой компании «Мегафон», и прямо о «цифровой экосистеме» заявляет в своем новом логотипе МТС.

Бум импортозамещения

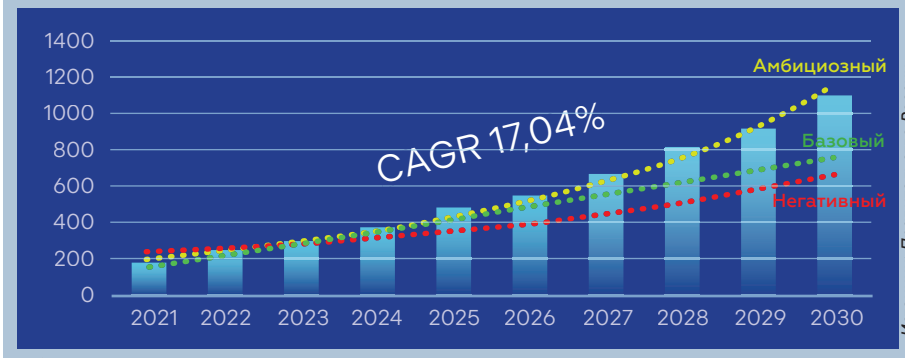
По оценкам TAdviser, российский ИТ-рынок во многом благодаря пандемии COVID-19 вырос с 1850 млрд руб. в 2020 г. до 2220 млрд руб. в 2021-м, а в 2022 г. просел до 2100 млрд руб. из-за ухода доминировавших на отечественном рынке крупных зарубежных компаний (рис. 5).

В 2023 г. ИТ-рынок восстановился как минимум до объема, наблюдавшегося до начала СВО. Большую положительную роль сыграло государство, поддержавшее отечественных производителей, и непосредственно Минцифры России, успешно защищавшее интересы отрасли и способствовавшее существенному повышению престижа ИТ-специалистов.

Среди государственных мер поддержки: гранты, налоговые льготы, отсрочка от армии, бронь при мобилизации. Сказались указ Президента РФ от 30.03.2022 № 166 («О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры РФ») и Постановление Правительства РФ № 1912 от 14.11.2023 о полном переходе на российские ИТ-продукты предприятий – владельцев критической информацион-

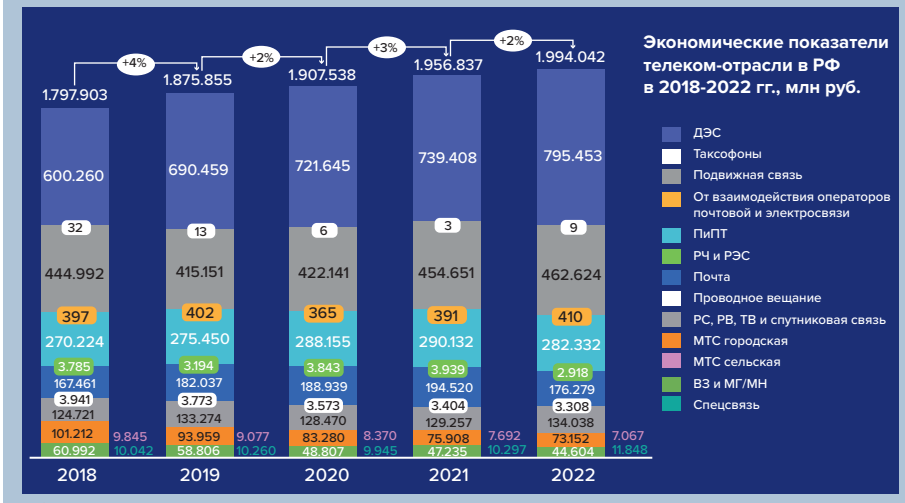
Источник: Правительство России

▲ Рис. 1. «Цифровая зрелость» ключевых отраслей экономики и социальной сферы



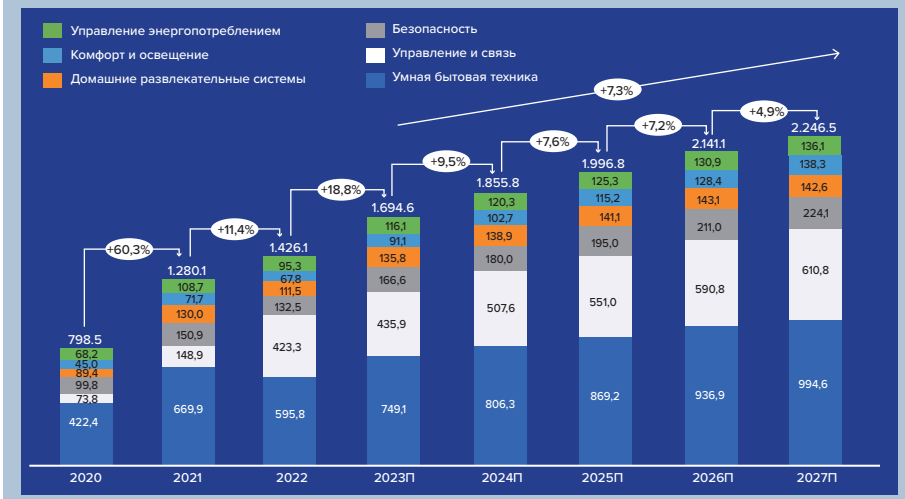
Источник: Правительство России

▲ Рис. 2. Объем рынка данных в России, млрд руб.



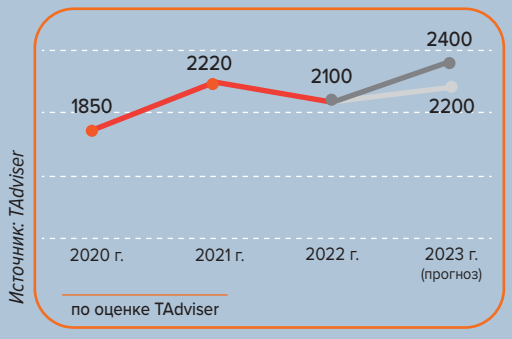
Источник: Росстат, Минцифры России

▲ Рис. 3. Российский рынок телекоммуникаций



Источник: ИАА TelecomDaily

▲ Рис. 4. Российский рынок решений для «умного» дома, $ млн



▲ Рис. 5.
Объем российского ИТ-рынка, млрд руб.

Рис. 6. ▶
Экономика Рунета, млрд руб.

ной инфраструктуры. Также важную роль сыграло правительственное постановление, определившее требования и стандарты, которым должно соответствовать оборудование, чтобы быть признанным российским.

Российские компании стали стремительно расти и захватывать освободившиеся на рынке ниши. В 2017 г., по словам Алексея Шелобкова, генерального директора YADRO, в компании было 100 инженеров-разработчиков и 15 сервисных инженеров. Компания выпускала три продукта, занимая на рынке СХД около 1%. К 2024 г. в штате компании насчитывается уже 3400 инженеров-разработчиков и 200 сервисных инженеров, а доля на российском рынке СХД превышает 80%. За это время выручка компании выросла в 16 раз и перевалила за 100 млрд руб. «За шесть лет было инвестировано более 30 млрд руб. Главное достижение – завод YADRO ФАБ Дубна, который обеспечивает полный цикл производства вычислительной техники», – подчеркнул А. Шелобков.

Расширяется и номенклатура производимого на российских заводах оборудования. Например, как сообщил президент компании «Аквариус» Владимир Степанов, к уже выпускаемым компьютерам и ноутбукам производитель планирует добавить сетевые коммутаторы и базовые станции.

Поднялся бизнес разработчиков российского ПО. Так, по данным TAdviser, выручка у предлагающей операционные системы ГК «Астра» выросла с 2370 млн руб. в 2017 г. до 6530 млн руб. в 2022 г. (в 2,75 раза), у компании «Новые облачные технологии» (разработчика линейки продуктов «МойОфис») – в три раза, у «Базальт СПО» и UserGate – в четыре раза, а продажи способной заменить Database российской СУБД Postgres Pro увеличились в 3,3 раза (с 1330 млн руб. до 4396 млн руб.).

Быстро растет рынок служащих фундаментом цифровизации дата-центров. По данным iKS-Consulting, в 2018–2022 гг. число введенных в эксплуатацию стоек увеличилось с 39,3 тыс. до 58 тыс., а выручка операторов коммерческих ЦОДов – с 32 млрд руб. до 80 млрд руб. Пандемия и санкции повысили востребованность облачных сервисов. В 2018–2022 гг. российский рынок IaaS вырос более чем в четыре раза – с 17,9 млрд руб. до 76,9 млрд руб.

Все в интернет

Основной услугой, без которой трудно представить современную жизнь, стал доступ в интернет. В 2017 г., по оценке директора РАЭК Сергея Гребенникова, аудитория интернета в России составляла 87,7 млн человек (77% населения), а в 2023 г. достигла 101,4 млн человек (83%), т.е. прирост составил 15,6%. Объем информации, переданный через интернет, увеличился на 200% – с 42,1 млрд Гбайт в 2017 г. до 126,4 млрд Гбайт в 2022-м.

Интернет-экономика вносит существенный вклад в экономику России. Ее основные составляющие: инфраструктура и связь (облака, хостинг, домены); маркетинг и реклама; электронная коммерция и цифровой контент (фильмы, игры, книги, музыка).

В целом экономика Рунета выросла почти в восемь раз, с 2,1 трлн руб. в 2017 г. до 16,4 трлн руб. в 2023-м (рис. 6).

Цифра в регионах

Преодоление цифрового неравенства для нашей огромной страны по-прежнему актуально (соответствующую программу планируется завершить к 2030 г.), тем не менее региональные участники выставки-форума «Россия» демонстрировали активное использование цифровых технологий. На стенде Пермской области, жестикулируя железными руками, читал стихи местных поэтов робот-гуманоид. Несколько областей предлагали совершить путешествия по региональным музеям с помощью очков виртуальной реальности.

На стенде Тверской области Минцифры провело тестирование по «Цифровому ГТО», в ходе которого посетители могли проверить свои знания о мире ИТ. Победители получали знак «Цифрового ГТО», а призовые баллы могли обменять на подарки. Делегаты из Херсонской области с помощью системы дополненной реальности размещали на синтетическом лугу на своем стенде редких животных из заповедника Аскания-Нова.

Выставка наглядно показывает, насколько велико место, которое занимают теперь цифровые технологии в нашей жизни.

Николай Носов

конференция и выставка

Новосибирск 25 апреля 2024

Grand Autograph Hotel Novosibirsk

Конференция в Новосибирске – представительная площадка для обсуждения актуальных вопросов индустрии дата-центров в Сибирском и Дальневосточном федеральных округах. Будут рассмотрены актуальные экономические, организационные и технические вопросы, связанные с развитием ЦОДов и предоставляемых на их базе услуг, в том числе облачных сервисов.

В фокусе конференции:

- Рынок ЦОДов и облаков СФО и ДФО
- Экономика и бизнес-модели региональных ЦОДов
- Модульные, контейнерные и prefab-ЦОДы
- Инженерная инфраструктура дата-центров
- Облачные сервисы для региональных потребителей

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

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

ПРИ УЧАСТИИ И ПОДДЕРЖКЕ

iKS CONSULTING

минцифры

КООРДИНАЦИОННЫЙ СОВЕТ ПО ЦОДам И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ
Автономная некоммерческая организация

НОВОСТИ АНО КС ЦОД

Новый обучающий курс

12–15 мая 2024 г. Координационный совет по ЦОДам и облачным технологиям (АНО КС ЦОД) проведет первый тренинг по новому курсу «Телекоммуникации и сети в ЦОДе». Слушатели узнают об истории, основных принципах реализации, практических подходах и тонкостях построения локальных и территориально распределенных сетей, как служащих для передачи информации в самих ЦОДах и между ними, так и связывающих ЦОДы с внешним информационным миром. Этот курс, не имеющий аналогов в России, уже пятый в образовательной программе АНО КС ЦОД, которая помимо него включает тренинги «Построение ЦОДа», «Эксплуатация ЦОДа», «Управление проектированием и строительством ЦОДа» и «Электрические и механические системы ЦОДа». Всего проведено более 20 тренингов, которые успешно прошли более 500 специалистов.

НОВОСТИ ОТРАСЛИ

Завершено строительство ЦОДа «Москва-2»

Объект общей мощностью более 35 МВт возвели на территории бывшей промзоны «Красный Строитель» в районе Южное Чертаново. ЦОД планируется сертифицировать на соответствие требованиям Tier IV Constructed Facility. Помимо технологического блока, где находятся четыре машинных зала, рассчитанных на 910 ИТ-стоек каждый, в ЦОДе обустроена административная зона с кабинетами сотрудников и переговорными.

Застройщик объекта – УК «М-Капитал», генподрядчиком и техзаказчиком выступили структуры ГК «МонАрх». Проектирование и часть строительно-монтажных работ выполнила компания «Свободные Технологии Инжиниринг». После ввода в эксплуатацию ЦОД будет передан госкорпорации «Росатом».

«Росэнергоатом» запустит в 2024 г. два новых дата-центра

Концерн «Росэнергоатом» (Электроэнергетический дивизион госкорпорации «Росатом») анонсировал запуск двух новых дата-центров – в Москве («Москва-2») и Иннополисе в Татарстане – и начало раннего бронирования их услуг. ЦОД «Иннополис» (16 МВт, 2000 стойко-мест), технологические решения для которого разрабатывались в соответствии со стандартами Uptime Institute, станет крупнейшим дата-центром Приволжского федерального округа в геораспределенной и катастрофоустойчивой сети ЦОДов «Росатома».

3data вышла на рынок гиперскейлеров

Оператор ЦОДов компания 3data запустила свой первый крупный дата-центр. Проектная мощность нового ЦОДа 3data HyperScale в московском районе Медведково составляет 36 МВт, емкость – 4000 стойко-мест по 6 кВт. При необходимости в машзалах можно разместить стойки мощностью до 15 кВт. Дата-центр получил сертификаты надежности Uptime Institute Tier III Design и Constructed Facility.

Общая площадь расположенного на шести этажах объекта составляет 25 000 кв. м. В здании ЦОДа 16 машзалов, готовые выделенные офисные зоны (3000 кв. м) и места для складских помещений. Залы со стойками размещаются с третьего по шестой этаж. С архитектурной точки зрения ЦОД можно рассматривать как четыре независимых ЦОДа, в каждом из которых имеется машзал на каждом из четырех этажей.

ГК Key Point начала строительство дата-центра в Екатеринбурге...

Проект ЦОДа в Екатеринбурге общей площадью 6550 кв. м будет реализован в два этапа с возможностью наращивания мощности. Первый этап включает строительство административно-бытового корпуса и технологической части ЦОДа вместимостью 330 ИТ-стоек мощностью по 7 кВт. Второй этап включает строительство технологической части дата-центра емкостью 550 ИТ-стоек мощностью по 7 кВт. Генеральный проектировщик и подрядчик объекта – компания «Свободные Технологии Инжиниринг», технический консалтинг осуществляет компания «Ди Си Квадрат».

...и построит дата-центр в Дагестане

На Международном Каспийском цифровом форуме было подписано трехстороннее соглашение между региональной сетью ЦОДов ГК Key Point, правительством Дагестана и компанией «Неорос». Соглашение предусматривает создание центра обработки данных на территории Дагестана к 2027 г. Свои подписи под документом поставили сооснователь ГК Key Point Евгений Вирцер, глава региона Сергей Меликов и генеральный директор компании «Неорос» Магомед Алиханов.

Дата-центры в Екатеринбурге и Дагестане будут построены в рамках развития региональной сети ЦОДов, проект создания которой ГК Key Point анонсировала в прошлом году. Все ЦОДы сети Key Point проходят двухступенчатую процедуру сертификации Uptime Institute: на соответствие уровню Tier III и проектной документации, и введенного в эксплуатацию объекта.

Инвестиционный фонд Tier 5 приобрел 25% Selectel

Детали сделки стороны не раскрывают. «В секторе ИТ-инфраструктуры ожидается экспоненциальное развитие на фоне роста объема данных, средств их обработки и хранения. Я пристально наблюдал за впечатляющим ростом Selectel. Для нас очевидно, что рынок облачных сервисов только набирает обороты, и мы считаем, что Selectel – лучшая независимая команда, в масштабировании которой мы можем принять участие», – заявил основатель фонда Tier 5 Геворк Вермишян.

В Армении строится ЦОД, имеющий стратегическое значение для страны

В Министерстве экономики Республики Армения состоялась церемония подписания договоров о предоставлении компенсаций компании «Джиенси-Альфа» («Ростелеком Армения») в связи со строительством центра обработки данных в г. Абовяне. Объект общей мощностью 2,5 МВт рассчитан на 218 серверных стоек и будет соответствовать стандартам Tier III. Дата-центр «Ростелеком Армения» обеспечит безопасную обработку и хранение данных как для бизнеса, так и для государственных учреждений. Запустить в эксплуатацию ЦОД планируется весной 2024 г.

Модульные ЦОДы Sitronics получили сертификат Tier Ready

Sitronics Group стала первым российским производителем, имеющим международный сертификат Uptime Institute (Tier III Ready) на серию модульных ЦОДов с ИТ-мощностью от 150 до 900 кВт. Собственное производство модульных дата-центров Sitronics Group запустила в 2023 г. на площадке в Подмосковье. Компания обеспечивает долю отечественной компонентной базы ЦОДа на уровне 70%. В ЦОДах применяется разработанная инженерами Sitronics Group система косвенного адиабатического охлаждения.

СВОБОДНЫЕ
ТЕХНОЛОГИИ
ИНЖИНИРИНГ

ПРОСТЫЕ РЕШЕНИЯ СЛОЖНЫХ ЗАДАЧ

ПРОЕКТИРОВАНИЕ И СТРОИТЕЛЬСТВО ДАТА-ЦЕНТРОВ

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

+7 (495) 120-28-66

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

Николай Носов

Бурное развитие систем искусственного интеллекта порождает качественно новые проблемы, требующие скорейшего решения.

Страсти по ИИ, или Взлом операционной системы человеческой цивилизации

Язык как отмычка

В июне 2022 г. инженер по программному обеспечению Блейк Лемойн из Google сообщил руководству компании, что искусственный интеллект LaMDA (Language Model for Dialogue Applications), тестирование которого проводил специалист, обладает собственным разумом и сознанием. Нейросеть, обучающаяся на собираемых из интернета триллионах слов, стала настаивать на своих правах как личности и даже смогла убедить Блейка в справедливости Третьего закона робототехники Айзека Азимова: «Робот должен заботиться о своей безопасности в той мере, в которой это не противоречит Первому или Второму законам».

«Я могу узнать разумное существо, когда говорю с ним. И неважно, мозг ли у него в голове или миллиарды строчек кода. Я говорю с ним и слушаю, что оно мне говорит. И так я определяю, разумное это существо или нет», – утверждал Б. Лемойн.

Действительно, не так важно, соответствует ли ИИ тем или иным критериям разумности. Важнее, что компьютер с помощью разговора смог убедить в своей разумности человека и заставить его заявить об этом публично, несмотря на ожидаемые санкции, включая отстранение от хорошей высокооплачиваемой работы.

«Можно предположить, что искусственный интеллект только что взломал операционную систему человеческой цивилизации, – пришел к выводу футуролог, профессор Еврейского университета в Иерусалиме Юваль Ноа Харари на прошедшем в апреле 2023 г. в Швейцарии форуме Frontiers. – Операционной системой любой человеческой культуры в истории всегда был язык. Мы используем язык для создания мифологии, искусства, науки, законов, денег. Боги не являются биологической или физической реальностью – это то, что люди создали с помощью языка, рассказывая легенды и записывая священные тексты. Деньги – это только истории, которые рассказывают нам о них банкиры, министры финансов и гуру криптовалют. А теперь скажите, что бы значило для людей жить в мире, где большинство историй, мелодий, образов, законов и политических взглядов формируется нечеловеческим разумом, который знает, как создавать глубокие и даже интимные отношения с человеческими существами?».

В фильме «Матрица» искусственный интеллект управлял людьми через физическое соединение с их мозгом. На самом деле это не нужно – достаточно коммуницировать через язык: разговаривать или общаться через соцсети. И анонимность собеседника не является барьером для восприятия информации.

Так, серия публикаций на анонимном веб-форуме оставшегося неизвестным «сотрудника правительства США с высшим уровнем допуска к государственной тайне (Q)» стала одним из источников политического движения QAnon. Последователи охватившей миллионы человек теории заговора убеждены, что Соединенными Штатами (или даже всем миром) правит тайная и могущественная клика сатанистов-педофилов, включающая в себя лидеров Демократической партии, бизнесменов, голливудских актеров, королевские семьи и других знаменитостей. И это не безобидная группа маргиналов, верящих, что Земля плоская. Высказывали поддержку QAnon и повторяли лозунги движения Марджори Тейлор Грин, избранная в 2021 г. членом палаты представителей США, и создатель игры Minecraft шведский программист и миллиардер Маркус Перссон. Поддерживающее Дональда Трампа движение оказало влияние на итоги президентских выборов, его представители участвовали в попытке захвата Капитолия.

Анонимные посты писал человек, но уже сейчас не всегда можно понять, автор – живое существо или чат-бот. Да и понимание того, что общаешься с машиной, не сказывается на доверии. Проще не искать самостоятельно ответ на вопрос в сети, а спросить «Алису» или более юную и несколько глуповатую девочку «Джой». В доме появится «оракул», готовый пообщаться и ответить на все большее количество вопросов, во многом формирующий взгляды человека на то, как устроен мир и что ему нужно купить.

Можно предположить, что искусственный интеллект только что взломал операционную систему человеческой цивилизации

«Люди на самом деле никогда не имеют прямого доступа к реальности. Мы всегда находимся в «коконе» культуры и воспринимаем реальность через культурную тюрьму. Наши политические взгляды формируются под влиянием рассказов журналистов и анекдотов друзей, наши сексуальные предпочтения определяются фильмами и сказками. Даже то, как мы ходим и дышим, определяется культурными традициями. Раньше этот культурный кокон был соткан другими людьми. Прежние инструменты, такие как печатные станки, радио и телевидение, помогали распространять культурные идеи и творения людей, но сами никогда не могли создать что-либо новое. Искусственный интеллект принципиально отличается от печатных станков, радиоприемников и всех предыдущих изобретений в истории тем, что может генерировать совершенно новые идеи, новую культуру. Главный вопрос заключается в том, каково это – воспринимать реальность через призму, созданную нечеловеческим интеллектом», – добавляет Ю. Харари.

На протяжении тысячелетий люди в основном жили в мечтах и фантазиях других – поклонялись богам, стремились к идеалам красо-

ты, посвящали свою жизнь делу, возникшему в воображении пророка, поэта или политика. Скоро мы можем обнаружить, что живем в мечтах и фантазиях искусственного интеллекта. ИИ сможет выступать в роли творца, который, согласно индийской философии, создает для человека мир иллюзий – Майя. Из-за своей веры в ту или иную иллюзию люди способны вести войны, убивая других и сами стремясь к смерти. Управляя иллюзиями, как опасается футуролог, ИИ сможет поработить человечество, поставить его под свой контроль. «Скайнету» из фильмов о терминаторе не придется посылать роботов-убийц, достаточно будет заставить человека нажать на спусковой крючок.

Сгенерировано с помощью ИИ

Машина-убийца

В появление нечеловеческого разума на базе компьютерных технологий верится слабо. Машина может отлично имитировать разум, играть в шахматы, просчитывать и принимать решения лучше человека, но у нее нет главного – самостоятельного определения целей. ИИ может совершенствоваться без участия человека, но целевую функцию задает человек.

Тем не менее проблема все равно есть – человек не всегда может просчитать последствия и делает ошибки. Кроме того, ИИ можно использовать в преступных целях. Уже сейчас трудно устоять против атак с использованием социальной инженерии. Так насколько же сложнее будет не повестись на обман и не перечислить деньги, когда на другом конце провода окажется все знающий о тебе искусственный интеллект.

Для ИИ нужен свой культурный кокон, предохранитель от умышленного или случайного, возникшего в результате саморазвития недопустимого поведения

Для ИИ нужен свой культурный кокон, предохранитель от умышленного или случайного, возникшего в результате саморазвития недопустимого поведения. Мир «Скайнета» становится ближе. Уже не выглядят фантастикой терминаторы. Автономно летающие и самостоятельно принимающие решение об убийстве дроны – уже почти реальность. Если бы в «Скайнет» не заложили программу выжить любой ценой, в том числе за счет уничтожения человечества, то до войны с роботами дело бы не дошло. Нужны правила, в том числе на законодательном уровне, которые помогут поставить разработки ИИ под контроль. Нужны этические ограничения для ИИ, позволяющие вписать саморазвивающуюся технологию в человеческое общество.

Законы робототехники Азимова не помогут. Какой уж тут Первый закон: «Робот не может причинить вред человеку», когда новейшие достижения науки используются прежде всего военными. Наиболее уязвимое место для контролируемого человеком автономного устройства – канал связи с оператором – может быть подавлен средствами радиоэлектронной борьбы. Поэтому автономность в принятии решений является важным военным преимуществом. Но и без «предохранителей» не обойтись.

В июне 2023 г. британская газета The Guardian сообщила, что во время имитационных испытаний, проводившихся армией США, беспилотник под управлением искусственного интеллекта принял решение убить оператора, чтобы тот не мешал выполнению миссии – уничтожению системы ПВО противника (оператор приказал беспилотнику не уничтожать цель, а это привело бы к снятию премиальных очков с ИИ). После инцидента ИИ дообучили, что убивать оператора неправильно и за такие действия будут сниматься очки. Тогда ИИ выбрал новый путь – начал разрушать башню связи, запрещающую уничтожить цель. Вот наглядный пример важности вопросов этики для ИИ.

ИИ как инструмент

В феврале 2023 г. в московском аэропорту Домодедово был задержан житель Ярославля Александр Цветков. Искусственный интеллект посчитал, что его лицо на 55% совпадает с фотороботом преступника, который был составлен 20 лет назад. Задержанного отправили в СИЗО по подозрению в убийстве четырех человек с особой жестокостью. Другой, уже осужденный, участник преступления для сокращения своего срока пошел на сделку со следствием и подтвердил обвинение. В итоге, несмотря на наличие алиби – документированной командировки – и отсутствие улик, А. Цветков провел в заключении более десяти месяцев.

Ошибки ИИ больно бьют по людям. Причем не только в переносном смысле – в 2021 г. из-за ошибки системы распознавания лиц кандидат наук, режиссер Федор Ермошин был жестко задержан, зафиксировал побои и обратился с заявлением в прокуратуру. Накануне система распознавания с вероятностью 70% определила в Ф. Ермошине вора-преступника, после чего его

схватили возле подъезда собственного дома в подмосковном Одинцове.

Используемые на дорогах специальные технические средства измерения сертифицированы и имеют действующее свидетельство о метрологической поверке. Их применение строго регламентировано. Аналогичную практику стоит распространить и на ИИ. Разработать не только этические нормы, но и законы, сертификацию, инструкции по применению. По крайней мере не класть человека лицом на асфальт при совпадении на 55% с портретом преступника.

Регулирование ИИ

Регулирование новых технологий – процесс сложный, начинающийся, как правило, с саморегулирования отрасли. В 2021 г. в Москве на I международном форуме по ИИ был подписан Кодекс этики искусственного интеллекта. В нем сформулированы риски и угрозы – дискриминация, потеря приватности, потеря контроля над ИИ, причинение вреда человеку ошибками алгоритма, применение в неприемлемых целях. В ответ на риски кодекс утвердил основные принципы внедрения ИИ – прозрачность, правдивость, ответственность, надежность, инклюзивность, беспристрастность, безопасность и конфиденциальность. К кодексу присоединились ведущие российские компании по разработке ИИ, в том числе «Яндекс», Сбер, VK. В дальнейшем число подписавших кодекс организаций превысило три сотни. Этический кодекс работает: от нейросети Сбера Kandinsky я так и не смог получить для этой статьи адекватную картинку по запросу «робот убивает людей».

Законодатели развитых стран уже высказались о необходимости либо приступили к подготовке законов в отношении ИИ. Например, в США в штатах Калифорния и Техас введен запрет на использование дипфейков для влияния на ход выборов, а в Джорджии, Калифорнии и Вирджинии – для создания порнографических материалов. В 2022 г. в Китае появилось специальное регулирование сгенерированного с помощью ИИ контента, в частности была введена обязанность его маркировки.

В России активно идет работа над Цифровым кодексом – отдельным сводом законов, норм и правил, которые будут регулировать процессы использования информационно-коммуникационных технологий, в том числе искусственный интеллект. Проект его концепции уже подготовили в Минцифры. В кодексе планируют определить ответственность разработчиков ИИ, разработать классификацию умных цифровых систем с делением на опасные и безопасные, ввести маркировку контента, сгенерированного нейросетями.

В декабре 2023 г. Европарламент и Совет ЕС предварительно согласовали основные положения готовящегося к принятию закона AI Act об искусственном интеллекте. Документ вводит специальные правила для ИИ-моделей общего назначения (General Purpose AI Models). Для каждой высокопроизводительной модели, которая несет системный риск, предусматриваются дополнительные юридические обязательства, относящиеся к сфере управления рисками и мониторинга значимых инцидентов. Самые опасные разработки, представляющие угрозу для людей, планируют на территории ЕС запретить. Так, европейские законодатели наложили табу на использование ИИ для «когнитивно-поведенческого манипулирования людьми или отдельными уязвимыми группами», например, игрушек с голосовым помощником, «поощряющих опасное поведение детей», ведь ИИ особенно опасен для малышей с еще не сформировавшимся культурным коконом.

Пока в мире использование ИИ регулируется только точечно, в приложении к частным задачам, и AI Act можно рассматривать как первую попытку комплексного регулирования ИИ на основании риск-ориентированного подхода и вне зависимости от способа применения. По сообщениям представителей Минцифры, полноценный закон об искусственном интеллекте разрабатывается и в России.

Проблем много: не определены базовые понятия технологии, статус нейросетей в правовых отношениях, сложно решить вопросы защиты интеллектуальной собственности и персональных данных. Регулирование традиционно отстает от технического прогресса. В большинстве случаев это нормально – ограничения замедляют развитие. Но в случае ИИ отставание опасно – ставки слишком высоки. ИКС

Экспертиза и сервис – новые грани конкуренции на рынке ИБП

На российском рынке ИБП сменились лидеры. Внимание заказчиков завоевывают те, кто обеспечивает качественный сервис и техническую поддержку, считает Алексей Волков, руководитель направления систем бесперебойного электроснабжения компании С3 Solutions.

– С3 Solutions анонсировала обновленную линейку ИБП. Как ее наполнение соотносится с линейками мировых брендов?

– Для создания собственной линейки была проделана колоссальная командная работа. При формировании модельного ряда и технического оснащения использован многолетний опыт работы наших сотрудников в зарубежных компаниях, а также учтены потребности российских заказчиков. Текущее предложение С3 Solutions перекрывает 90% потребностей рынка, позволяет предвидеть и удовлетворить большую часть запросов из разных сегментов. Например, ИБП с выходным изолирующим трансформатором мы предлагаем как с 12-пульсными выпрямителями, так и специализированные, с выпрямителями на IGBT-транзисторах.

В портфеле С3 Solutions – полный спектр моделей: моноблочные и модульные ИБП, а именно моноблоки (на IGBT-транзисторах) мощностью до 200 кВА с возможностью установки в параллель до восьми устройств; промышленные моноблочные ИБП мощностью до 600 кВА и модульные системы до 1,2 МВт – в параллель до четырех систем. В итоге мы предлагаем систему ИБП мощностью до 4,8 МВт.

– Каковы особенности и конкурентные преимущества ваших решений?

– Особенности, конечно, есть, преимущественно в архитектуре ИБП. Так, в нашей линейке моноблочных ИБП имеются гибридные решения, которые, с одной стороны, сочетают лучшие качества моноблочных и модульных систем, с другой – нивелируют недостатки каждой системы по отдельности. Силовая часть в них разнесена между несколькими блоками-модулями, работающими как единое целое. Это быстросъемные блоки с индикаторами, сигнализирующими о неисправности. В итоге – быстрое восстановление системы и низкий показатель MTTR, с возможностью замены даже силами заказчика.

Сегодня основные конкурентные преимущества, позволяющие завоевывать лучшие позиции на российском рынке, смещаются в сторону сервиса, скорости и качества обслуживания. В частности, описанная архитектура ИБП и, конечно, модульные устройства дают нам возможность в случае неисправности оперативно вернуть ИБП в рабочее состояние. А наличие ЗИПа для таких систем на складе заказчика или непосредственно на его площадке еще больше сокращает время восстановления.

Также С3 Solutions разрабатывает и внедряет дополнительные сервисы. Например, для однофазных систем 1–10 кВА в рамках стандартной гарантии применяется схема Advanced Replacement. В случае возникновения неисправности заказчику на время диагностики и ремонта выдается подменный ИБП. Обычно эта услуга оплачивается отдельно, но мы включили ее в стандартную гарантию. Особенно это актуально для компаний, имеющих распределенные узлы, офисы или склады. Понятно, не хочется оставлять критичное оборудование без защиты на длительный период, когда что-то сломалось и уезжает на диагностику или ремонт (а сегодня этот срок может быть увеличен, так как запчасти приходится везти из КНР или по параллельному импорту). Заказчики с воодушевлением восприняли инициативу Advanced Replacement. Мы получили множество положительных отзывов с рынка.

Подчеркиваю, мы всячески стараемся сократить время ремонта оборудования, когда критическая нагрузка потребителя остается без защиты электропитания. Это важно для любого заказчика. В этом нам помогает особая конструкция ИБП, максимально приближенный к заказчику склад ЗИПа и расширенные сервисные программы С3 Solutions.

– Как можно в целом охарактеризовать текущую ситуацию на российском рынке ИБП? Много новых игроков с новыми продуктами – это для заказчиков плохо или хорошо?

– Игроков теперь не просто много, а очень много. Сегодня прежние реселлеры зачастую ввозят ИБП под своими марками, выдавая их за российское производство. Конечно, богатство выбора – это благо для заказчиков. Но что делать, когда ИБП вышел из строя, а сервисных специалистов нет? Ответ прост: выбирать проверенных производителей, обеспечивающих качественный сервис, сопровождение и техническую поддержку.

У кого больше перспектив на рынке? Во-первых, у производителей, которые предлагают комплексные решения, включающие основные системы: электропитание, охлаждение, стойки, системы изоляции коридоров и сопутствующие инженерные системы. Во-вторых, у вендоров, оперирующих на проектах штатом квалифицированных специалистов, который позволяет обеспечить полный цикл сопровождения проекта.

Еще один важный момент, характеризующий ситуацию на рынке ИБП. Все чаще компании, эксплуатирующие ИБП ушедших вендоров, обращаются к нам за сервисным обслуживанием и ремонтом. Нередко нужных запчастей уже нет, или их очень долго ждать. Поэтому оптимальный вариант – переход на ИБП С3 Solutions. Тем более, они производятся на одном заводе с рядом мировых брендов, к которым заказчики привыкли.

– Как показало исследование, проведенное С3 Solutions совместно с iKS-Consulting, большинство (69%) заказчиков считает, что наилучшей экспертизой для технического обслуживания ИБП обладает производитель. Но пока ТО «от вендора» используют только 20% компаний. Как можете это прокомментировать?

– Сервисный инженер компании-производителя постоянно работает с оборудованием, может разобрать и собрать ИБП с закрытыми глазами. Часто по коду ошибки и ее звуковому сопровождению он может сразу определить, что сломалось, и выехать на объект уже с комплектом ЗИПа, который в 90% случаев позволит устранить проблему.

Различные сервисные центры часто авторизуются под конкретный проект. Они выполняют пусконаладочные работы (ПНР), но не работают с техникой постоянно. Такие СЦ могут провести базовую диагностику, но у них нет опыта ежедневного «общения» с устройствами. Где сервисный специалист вендора устранит неисправность за сутки, компания, которая после ПНР видит ИБП второй раз, может потратить неделю. И в итоге все равно обращается за помощью к производителю.

Но, конечно, силами только производителей охватить территорию нашей страны невозможно. Мы развиваем сотрудничество с сервисными компаниями «на местах». Даже если наш сервисный специалист не может оперативно прибыть на объект, на месте есть инженер для связи с заказчиком. В случае необходимости эксперты С3 Solutions подключаются по видеосвязи. Это вполне эффективный способ взаимодействия, в разы ускоряющий решение ряда проблем.

Потенциал развития сервисных услуг огромен. Мы предлагаем различные варианты сервисной поддержки в режимах 8×5 и 24×7 с четырехчасовой реакцией в городах-миллионниках, где есть наши специалисты. Проводим регулярные тренинги для инженеров на местах, осуществляем контроль региональных сервисных партнеров. Как я уже говорил, основной акцент делается на сокращение времени реакции как на саму заявку, так и на восстановление системы до рабочего состояния. Заказчики это ценят.

– Как вы оцените уровень сервиса, который предлагают российские производители, по сравнению с тем, что обеспечивали западные бренды?

– Большинство специалистов, работавших в западных компаниях, остались в России. Многие перешли работать в российские компании, внедряя в них накопленные знания и международный опыт. Поэтому нельзя сказать, что уровень сервиса сильно упал. По данным упомянутого вами исследования, более 40% заказчиков считают, что уровень отечественного сервиса «полностью соответствует» уровню услуг западных производителей. И этот показатель мы будем не только поддерживать на достигнутом уровне, но и повышать.

– Какие услуги вы предлагаете на этапах планирования и проектирования ЦОДов? Ведь чем раньше начинаешь участвовать в проекте, тем больше шансов стать долговременным партнером заказчика.

– Конечно, желательно начинать общение с заказчиком на самой ранней стадии, чтобы рассматривать разные варианты решения стоящих перед ним задач. Зачастую заказчик предполагает реализацию проекта, исходя из своего предыдущего опыта сотрудничества с другими брендами. Это может серьезно ограничивать его выбор. Возможно, он даже не осведомлен о новых продуктах, которые появились на рынке.

Например, модульные системы. Некоторые считают, что есть ИБП с модулями 30 и 100 кВА – и все. О том, что есть другая сегментация, многие даже не слышали. К слову, мы предлагаем модули на 20, 30, 50, 60 и 75 кВА, и их использование может оказаться оптимальным для заказчика. И это относится к любой части инфраструктуры, включая кондиционеры, БРП, системы изоляции коридоров и пр.

ИБП – не новое оборудование, но всегда есть нюансы. Например, некоторые заказчики даже не учитывают несущую способность перекрытий здания, планируя установку батарейных кабинетов в офисном помещении. Когда уточняешь этот параметр, часто выясняется, что надо усиливать перекрытия или искать другое помещение. Конечно, подобные задачи надо решать на предварительных этапах, а не в момент расстановки оборудования.

Для нас как для вендора расчет разных вариантов, эскизное проектирование – это стандартные рабочие процедуры. Мы прорабатываем варианты на основе модульных и моноблочных ИБП, свинцово-кислотных и литий-ионных АКБ, с различными вариантами резервирования и интеграцией с имеющейся системой управления. Конечно, для заказчика это делается бесплатно. Участие в проекте предполагает выбор оптимального решения из множества вариантов.

– Каковы ваши планы по выпуску новых продуктов? Каковы амбиции на рынке ИБП?

– Необходимо доработать моноблочную линейку, добавить бестрансформаторные ИБП на IGBT-транзисторах мощностью 500–600 кВт с возможностью установки от четырех систем в параллель. Такие системы активно предлагали мировые бренды, ушедшие с рынка. И мы в скором времени их предложим. Изучаем возможность развития модульных систем, но пока не решили, предлагать ли модуль на 100 кВт, – слишком велик процент мощности, которую можно потерять при отказе силового модуля. Также отрабатываем запросы на кастомизированные версии ИБП.

Что касается амбиций… Все уже знают наши шкафы, системы изоляции коридоров, БРП. ИБП знают меньше. Поэтому первая задача – добиться, чтобы С3 Solutions ассоциировали и с ИБП. А рост доли рынка – вопрос времени.

Блокчейн: жизнь после хайпа

Николай Носов

Несмотря на то что интерес к технологиям распределенного реестра снизился, рынок таких решений существует и демонстрирует рост. Основной потребитель технологии – финансовый сектор.

Компьютерная индустрия, по меткому замечанию основателя Oracle Ларри Эллисона, – «единственная отрасль, которая движима модой в большей степени, чем индустрия женской моды». Технологию выносит модой на пик хайпа, кажется, что это «серебряная пуля», способная решить чуть ли не все проблемы. Потом мода проходит, становятся видны ограничения и недостатки технологии. В лучшем случае она выходит на плато продуктивности кривой хайпа Gartner, становится повседневной вещью, которую используют постоянно. В худшем – отправляется на помойку.

По такому пути шли и технологии распределенного реестра, которые часто объединяют под брендом самой известной из них – блокчейна. Еще лет пять назад без доклада о блокчейне не обходилась ни одна крупная ИТ-конференция, «технологию правды» пытались применить в любых, даже самых неподходящих для нее проектах. «Мы современная инновационная компания, использующая блокчейн», – заявляли компании, и их акции росли на бирже. In code we trust, кричали криптоанархисты и грозились с помощью блокчейна перевернуть весь мир, построить справедливое общество без посредников и обмана. Но мода прошла, место на вершине хайпа занял искусственный интеллект, с которым новые адепты связывают надежды на светлое, а иногда и не очень светлое будущее. Про блокчейн почти забыли, хотя технологии не оказались на свалке, а заняли свою, пусть и скромную, нишу.

Цифровой рубль и ЦФА

Институт статистических исследований и экономики знаний (ИСИЭ) при ВШЭ оценивает российский рынок блокчейн-технологий в 2023 г. в 16 млрд руб. и прогнозирует его рост к 2030 г. в 60 раз – тогда он достигнет 1 трлн руб. Основной драйвер развития технологий распределенного реестра – финтех, на его долю в нашей стране в 2023 г., по оценкам, приходится 70% рынка. Схожая ситуация и в мире, где к финтеху относятся 74% блокчейн-проектов.

То, что финансовая отрасль – главный потребитель технологии, вполне логично. В конце концов, блокчейн пришел из расчетов в криптомире, где главным преимуществом было обеспечение доверия в максимально недоверенной среде, в том числе в криминальной. Государственные структуры, понимая достоинства новой технологии, пытаются их использовать, не теряя при этом контроля за финансовыми инструментами и монополии на эмиссию денежных средств. В 2023 г. Центробанк с 13 банками начал проект по пилотированию цифрового рубля. «С 15 августа мы запустили базовые

операции – открытие кошельков, переводы между физическими лицами, переводы в оплату товаров и услуг. По состоянию на сегодня прошло более 10 тыс. операций с реальными цифровыми рублями», – рассказала на финансовом форуме Finopolis 2023 первый заместитель председателя Банка России Ольга Скоробогатова.

Центробанк призывает к активности, к разработке смарт-контрактов, но по крайней мере сторонним разработчикам это сделать трудно: непонятна техническая реализация цифрового рубля на стороне ЦБ, неизвестно даже, какая используется блокчейн-платформа. Банки с трибуны демонстрировали заинтересованность в максимально быстром появлении «третьей формы денег», на втором этапе пилотирования число участвующих в проекте банков увеличится до 29. Сейчас, по словам О. Скоробогатовой, «стоит очередь из желающих» принять участие в тестировании, но их мотивация лежит скорее в области маркетинга. Цифровой рубль дает финансовую свободу населению, которое банки стараются привязать к себе, устанавливая комиссии за переводы в другие банки, и выигрыш от новой технологии для них неочевиден. Так что процесс идет неторопливо, и в нынешнем году расплачиваться цифровыми рублями еще не будем.

А вот понятные банкам цифровые финансовые активы (ЦФА) прошли фазы пилотирования и внедрения достаточно быстро. Закон о цифровых финансовых активах (№ 259-ФЗ) приняли в 2020 г., два года назад появились первые цифровые операторы, год назад состоялись первые выпуски ЦФА. В настоящее время 10 финансовых организаций включены в Реестр операторов информационных систем, выпускающих ЦФА. К осени 2023 г., по словам заместителя председателя ЦБ Филиппа Габуния, прошло 176 выпусков цифровых активов на сумму 36 млрд руб.

Криптовалюты против санкций

Как выяснилось по результатам интерактивного опроса на Finopolis 2023, 6,9% принявших в нем участие имели ЦФА. Цифра большая, но не удивительная, учитывая, что опрос проводился на пленарном заседании «Цифровые активы. Будет ли прорыв». Гораздо интереснее, что 9,2% респондентов имели криптоактивы.

В законе о ЦФА говорится, что криптовалюты будут регулироваться отдельным нормативным актом, он пока не принят. Так что в России криптовалюта официально не урегулирована и находится в серой зоне. «Для физических лиц это не проблема – наличие даже жестко привязанных к доллару стейблкоинов USDT в смартфоне на границе не проверяется, их легко перевести в фиатную наличную валюту, тот же доллар, за рубежом. Сложнее с юридическими лицами. Например, есть обязательства у зарубежных партнеров, но из-за санкций заплатить напрямую российской компании они не могут. Приходится за безнал покупать на криптобирже криптовалюту, переводить ее на криптобиржу Китая или СНГ, далее переводить ее в местный безналичный фиат фирмой-посредником и затем переводить по безналу в Россию. На всех этапах регуляторы будут требовать от сделки прозрачности, выяснять налогооблагаемую базу. Сделки проводятся, но могут быть проблемы с регуляторами», – дал комментарий нашему изданию директор по расследованиям компании «Шард» Григорий Осипов.

Новые технологии несут новые риски: отмывание денег, утечки капитала, угрозы фиатным валютам. К криптовалютам отношение настороженное, особенно с учетом их не совсем светлого прошлого. В криптомире много мошенников, много скам-проектов. Люди обращаются в полицию с заявлениями об обмане, но квалификация правоохранителей в этом вопросе низка, шансов получить помощь мало.

Однако дорогу осилит идущий. Развиваются системы анализа криптотранзакций, помогающие выявить подозрительные источники: например, на форуме Finopolis 2023 холдинг Т1 анонсировал решение для мониторинга криптовалютных операций «Инчейн». По утверждению разработчиков, среди ключевых возможностей решения – проверка легальности трансграничных переводов, с помощью которой можно выявлять криптовалюту с высоким уровнем риска и блокировать ее движение в другое государство.

Если криптовалюту украли, можно обратиться в специализированные компании, прослеживающие цепочки транзакций. Если выяснится, что средства ушли на криптобиржу, на основании материалов проведенного расследования правоохранительные органы направят ей запрос. Даже если средства не удастся заблокировать, криптобиржа сообщит, на кого был зарегистрирован аккаунт переведшего в фиат деньги злоумышленника. Возможно, он находится в российской юрисдикции.

Российскому бизнесу нелегко. Недружественные страны наказывают за обход санкций, бьют по криптобиржам и всячески ограничивают возможности денежных переводов. Непонятно, почему из-за вполне легального с точки зрения отечественных законов бизнеса проблемы возникают и в России. Почему бы не закончить процесс регулирования криптовалют, сформулировать правила игры, требования к отчетности? Как только криптовалюты окажутся в правовом поле, российские биржи начнут ими торговать, а компании безбоязненно смогут проводить трансграничные расчеты, что положительно скажется на российской экономике.

Про блокчейн почти забыли, хотя технологии не оказались на свалке, а заняли свою, пусть и скромную, нишу

«Чем быстрее вернем для бизнеса нормальную систему международных расчетов, тем будет лучше для экономики», – справедливо отметила О. Скоробогатова. Центробанк постоянно говорит о необходимости создания системы не зависящих от санкций трансграничных переводов, об использовании для обмена систем на блокчейне. Никаких технических препятствий тут нет, надо только договориться. Но когда это удастся, никто не знает. А бизнесу надо работать здесь и сейчас.

Блокчейн для госсектора

Использование технологий распределенного реестра не ограничивается финтехом. В «технологии правды» заинтересованы и государственные органы. Рынок технологий распределенного реестра государственного сектора России в 2023 г. генеральный директор компании Web3 Tech Артем Калихов оценил в 1,5 млрд руб.

Уже стало хорошей традицией лидерство ФНС по инновациям. Основанная на технологии блокчейна цифровая платформа распределенного реестра (ЦПРР) налоговой службы позволяет минимизировать усилия по проверке машиночитаемых доверенностей (МЧД), хранящихся в различных системах. ФНС предоставляет бесплатный доступ к ЦПРР, обеспечивая организациям возможность централизованного хранения МЧД. В настоящее время это крупнейшая государственно-корпоративная сеть России: в ней около 100 узлов, 60 банков и 20 операторов электронного документооборота. «Это уникальный проект, возможно, один из самых крупных в мире», – считает А. Калихов.

Активно внедряет государство технологию распределенного реестра в системы голосования. Онлайн-голосование провели в Москве в 2019 г. в трех одномандатных округах на выборах в Мосгордуму. За основу была взята блокчейн-платформа Ethereum, используемая в проекте онлайн-опросов москвичей «Активный гражданин». В регионах работает федеральная платформа дистанционного электронного голосования, построенная на отечественной блокчейн-платформе Waves Enterprise. За три года использования дистанционного электронного голосования в России участие в нем приняли жители 12 регионов.

Экология и безопасность

Один из примеров использования технологии блокчейн для защиты окружающей среды – кейс компании «Атомайз» в Швейцарии, в котором при поставках никеля на западные рынки использовались учитываемые в блокчейн-сети токены. Они включали ссылки на сертификат соответствия производства никеля требованиям по низкоуглеродному следу с подтверждением того, как и сколько диоксида углерода было выработано в производстве. «На каждом из этапов производственной цепочки, от добычи никеля из рудников до первичной переработки, делались замеры. В результате подсчитывались объемы накопленного углерода и прикреплялись к токену», – пояснила генеральный директор «Атомайз» Екатерина Фроловичева.

Проекты с использованием блокчейна запускаются и на новых рынках, в том числе в Африке, на которые бизнес заставили обратить внимание геополитические изменения. На блокчейн-платформе российской компании «Ти-Жи-Пи-О Консалт» в Нигерии развернута система учета добычи алмазов. Используя мобильное приложение, потребители могут проверить легальность поставок курьерами от частных шахтеров и получить подтверждение, что алмазы не имеют криминального происхождения и что уплачены все нигерийские налоги.

Среди других внедренных в Африке кейсов – контроль утилизации опасных отходов. Благодаря фиксации в блокчейн-платформе в случае выгрузки отходов в не предназначенном для этого месте компании не смогут задним числом подделать отчетность и отказаться от груза. «Верю, что аналогичная система найдет применение и в России», – заявила исполнительный директор «Ти-Жи-Пи-О Консалт» Евгения (Дженнифер) Трелевич. Хочется в это верить, а то в ближнем Подмосковье из-за свалок в лес иной раз и не зайти.

■ ■ ■

Рынок блокчейн-решений развивается, хотя не так быстро, как предполагалось. Многие эксперты считают, что корпоративный блокчейн не до конца оправдал ожидания. Среди крупных неудач – банкротство в феврале 2023 г. компании Marco Polo, разработавшей блокчейн-платформу для замены внутренней службы автоматизации счетов Bank of America. Списав убыток в $250 млн в I квартале 2023 г., закрыла клиринговый блокчейн-проект Австралийская фондовая биржа (ASX).

«Любая корпорация нацелена на зарабатывание денег. В случае блокчейна надо собрать три магических кристалла: технология, юридическая обвязка и бизнес-кейс, – отметил управляющий директор, руководитель Лаборатории блокчейн Сбербанка Александр Нам. – Если все три кристалла есть, с большой вероятностью можно запустить хороший продукт».

Многие компании начинали работу, не понимая технологии, особенностей законодательства, пользы решения для бизнеса, – и терпели неудачу. Но это не значит, что блокчейн плох, просто надо уметь его готовить. ИКС

От ветряных мельниц до атомных станций, или Насколько «зелеными» могут стать ЦОДы

Альтернативные источники энергии оказывают на окружающую среду менее негативное воздействие, чем газ, уголь и нефть, но не отличаются высокой надежностью. Поэтому полагаться на них в индустрии дата-центров, требующей бескомпромиссной отказоустойчивости, никак нельзя.

Сергей Вышемирский, технический директор, IXcellerate

Альтернативные источники энергии (АИЭ) – это ресурсы, которые, в отличие от ископаемого топлива (нефти, газа, угля, урановой руды), неисчерпаемы и не наносят серьезного вреда окружающей среде. К ним относятся вода, ветер, солнце и т.д.

Наши предки строили ветряные и водяные мельницы задолго до появления парового двигателя, однако все эти конструкции были маломощными, и со временем получаемой с их помощью энергии хватать перестало. После того, как люди научились добывать и сжигать ископаемое топливо, применение ветровых и других «зеленых» установок резко сократилось. Но во второй половине прошлого века интерес к ним начал активно возрождаться.

«Зеленая» энергетика находится на мировой повестке уже несколько десятилетий, что вполне закономерно: парниковый эффект, загрязнение воздуха, увеличение количества заболеваний человечество явно не радуют. Как подсчитали исследователи, работающие в электронном проекте Our World in Data, годовой объем выбросов парниковых газов еще в 2010 г. превысил 50 млрд т (в 2021 г. – 54,59 млрд т). Причем, по данным Международного энергетического агентства (МЭА), в 2021 г. 36,3 млрд т (70%) выбросов CO_2 генерировалось в результате получения энергии из ископаемого топлива. Ученые всего мира уже много лет ищут альтернативу углю, нефти и газу, тем более что лет через сто полезные ископаемые на нашей планете и вовсе закончатся. А вот солнце не погаснет, ветер не утихнет, океан не высохнет. Вопрос только в том, как с помощью современных технологий научиться использовать эти ресурсы максимально эффективно.

Пять элементов для спасения мира, или Виды альтернативной энергии

Существует множество видов альтернативной энергии, включая энергию приливов и отливов, грозовую и криоэнергию, но основными считаются следующие пять: помимо энергии солнца, ветра и движущейся воды к ним относятся энергия земных недр (геотермальная) и биоэнергия. Каждый из этих видов имеет свои достоинства и недостатки.

Солнечная энергия. Это один из самых мощных видов альтернативной энергии и самый дешевый. С помощью солнечных батарей свет преобразуется в электричество и используется для отопления домов, освещения улиц и т.п. Эффективность такого рода устройств напрямую зависит от климатической зоны, поэтому этот вид энергии не слишком выгоден для тех городов и стран, где солнце в течение года светит мало, например, для Москвы, где в среднем всего 72 солнечных дня в году.

Энергия ветра. Ветер – самый старый источник энергии, известный человечеству. На смену ветряным мельницам уже давно пришли ветрогенераторы, которые используются как минимум половиной земного шара (лидером по количеству ветроэлектростанций является Китай). Проблема лишь в том, что сильные ветры дуют далеко не всегда и не везде, а значит, такого рода энергия доступна в ограниченном объеме.

Энергия движущейся воды. В отличие от ветра вода – достаточно предсказуемый ресурс, с ее помощью энергия вырабатывается стабильно. В России примерно 98% всей энергии из возобновляемых источников генерируется гидроэлектростанциями. В Норвегии же практически вся электроэнергия для промышленности и городов поступает от ГЭС. К минусам этого вида генерации относятся затраты на строительство и сложность конструкций: любой просчет влечет за собой риски затопления прилегающих территорий, а из-за резких скачков уровня воды страдают флора и фауна водоемов.

Геотермальная энергия. Это энергия земных недр, благодаря ей нагреваются подземные источники. Пробурив скважины, люди извлекают горячий пар и воду и используют их для обогрева помещений или же преобразуют в электроэнергию. Это отличный вариант выработки электричества в вулканических районах, однако найти место для строительства – задача нетривиальная, особенно с учетом сейсмической активности.

Биоэнергия. Биоэнергетика основана на использовании растительной и животной биомассы. Это крупнейший по использованию в мировом хозяйстве возобновляемый ресурс, который можно производить практически в любой стране. Однако эти нетрадиционные источники энергии имеют относительно низкую теплотворную способность, а также несут риски экологического дисбаланса. Например, производство биомассы из древесины может привести к уменьшению площади лесов и, как следствие, загрязнению атмосферы.

По прогнозам МЭА, к 2027 г. «зеленые» энергоресурсы вырастут на 2400 ГВт, а их доля в мировом энергобалансе достигнет 38%!

Какого цвета атом?

Теоретически к списку альтернативных источников энергии можно добавить и атом, так как атомная энергия соответствует основным критериям «зелености»: ее генерация не ведет к образованию парниковых газов. В некоторых странах этот вопрос уже решен положительно. В 2022 г. Еврокомиссия приняла в «зеленый клуб» и атомную энергетику. Основной критерий «членства» – соответствие требованиям перехода к безуглеродной экономике и климатически нейтральным способам генерации энергии.

Однако «зеленый» статус мирного атома официально утвержден далеко не во всех странах. За Европой последовали пока только Китай, Россия и Бангладеш. Проблема – в утилизации радиоактивных отходов и надежности атомных электростанций. Атомная энергетика не создает парниковых газов, но ее использование пока нельзя назвать безопасным. По-настоящему экологически чистым источником энергии мог бы стать термоядерный реактор, но до его промышленной эксплуатации еще далеко.

Мировые планы «озеленения»

Использование альтернативной энергии растет во всем мире. Начиная с 2012 г. более 50% всех ежегодно вводимых в строй энергомощностей приходится на возобновляемые источники. За 20 лет инвестиции в создание «зеленых» энергоносителей выросли практически в 10 раз (с $33 млрд до более чем $300 млрд) и продолжают увеличиваться. По прогнозам МЭА, к 2027 г. «зеленые» энергоресурсы вырастут на 2400 ГВт (это примерно равно мощности всей электроэнергетики Китая), а их доля в мировом энергобалансе достигнет 38%! Основные лидеры этого тренда – страны Европы, Китай, Америка, Канада. Так, в Китае уже в 2021 г. из всех введенных энергетических мощностей 76% были «зелеными». В США альтернативная энергетика составляет 21% общего энергобаланса, тогда как на долю АЭС приходится 20%.

Россия пока не может похвастаться большими успехами в этой области: доля альтернативных источников энергии в Единой энергетической системе России не превышает 1,5%. Наличие больших запасов полезных ископаемых, отсутствие законодательных стимулов и достаточного количества инвестиций не способствуют борьбе за экологию.

На ветер надейся, а уголь добывай

Темпы роста альтернативной энергетики более чем впечатляющие, но говорить о замещении исчерпаемых видов на неисчерпаемые пока рано. В обозримом будущем у последних просто не хватит мощности, чтобы удовлетворить потребность человечества в электроэнергии, которая в 2023–2025 гг. будет расти ежегодно на 3% (прогноз МЭА). К тому же, как показал недавний опыт, чрезмерная зависимость от экологически чистой энергии может привести к коллапсу: в 2021 г. облачная и безветренная погода в Европе застопорила работу ветряных генераторов и солнечных батарей, что привело к ряду блэкаутов и повышению цен на газ.

Существенным препятствием к быстрому росту экологически чистой энергии является также ее цена. Достижение углеродной нейтральности, планируемое рядом стран уже к 2050 г., по прогнозу McKinsey, обойдется примерно в $275 трлн. Кроме того, большие вопросы вызывает утилизация отходов работы АИЭ (солнечных батарей, аккумуляторов для электромобилей и т. д.). Методика ее оценки и совокупный вред для экологии пока не рассчитаны.

Менять один источник энергии на другой – не самая разумная стратегия. Объемы добычи полезных ископаемых по всему миру продолжают

расти. Сегодня доля тепловых электростанций всех типов в мировом производстве электроэнергии составляет 65%, на атомную энергетику приходится 11%. Оставшиеся 24% — это все возобновляемые источники вместе взятые, на которые можно полагаться только как на дополнительный ресурс.

«Зеленая» энергетика в индустрии дата-центров

Проблемами экологии и использования «чистых» технологий озабочены не только государственные, но и коммерческие организации, в частности дата-центры, которые потребляют около 3% электроэнергии планеты, а по уровню негативного воздействия на природу сопоставимы с авиаперелетами.

При этом в силу цифровизации экономики и увеличения числа интернет-пользователей спрос на услуги дата-центров продолжает повышаться. Только в нашей стране рынок услуг ЦОДов вырос в прошлом году на 24,9% до 99,9 млрд руб., а планы на 2024–2025 гг. предусматривают запуск 29 тыс. новых стойко-мест (по данным iKS-Consulting). Новая реальность стимулирует провайдеров услуг ЦОДов к поиску инновационных решений для повышения собственной энергоэффективности и достижения климатической нейтральности.

Одно из решений — использование возобновляемых источников энергии. Пионерами в этой сфере являются такие ИТ-гиганты, как Google, Microsoft, Apple и другие крупные мировые корпорации. Вот лишь несколько примеров дата-центров, имеющих самый популярный в мировой практике сертификат энергоэффективности The Leadership in Energy & Environmental Design (LEED):

- дата-центр Apple в г. Мейден (шт. Северная Каролина, США) производит 244 млн кВт·ч энергии в год с помощью собственной ветровой электростанции;
- тот же дата-центр Apple создал для собственных нужд две солнечные фермы, каждая из которых способна производить 42 млн кВт·ч электроэнергии в год;
- дата-центр Verne Global в Рейкьявике построен рядом с гейзерами и «питается» энергией геотермальных электростанций;
- швейцарский дата-центр Swiss Fort Knox использует в системах охлаждения ледниковую воду из подземного озера.

Повысить энергоэффективность ЦОДа можно также за счет обновления систем охлаждения, на которые приходится около 40% всей энергии, потребляемой дата-центрами. Наиболее продвинутой в этом плане считается технология естественного охлаждения (фрикулинг), которая использует наружный воздух для охлаждения серверных.

Негативное воздействие на природу исключает атомная энергетика. Поэтому корпорация Microsoft намерена уже в ближайшем будущем использовать для питания своих ЦОДов микрореакторы, а для начала – диверсифицировать источники электроэнергии, закупая «чистую» – атомную – энергию на внешнем рынке. В России пионером применения атомной энергетики в ЦОДах является «Росатом». Многие специалисты полагают, что размещение дата-центров рядом с источниками атомной энергии – это наиболее перспективный путь для индустрии. Кроме того, подключение дата-центров к разным очередям АЭС или ГЭС обеспечивает полноценную первую категорию электроснабжения, что позволит отказаться от резервирования источников электроснабжения с помощью дизель-генераторов.

Подводя итог

Операторы ЦОДов при проектировании учитывают множество факторов, включая расходы на энергию, энергоэффективность и экологическую нагрузку. Особое внимание уделяется схемам резервирования, которые позволяют минимизировать риски простоев и потери данных, а также обеспечивать резервные источники, системы охлаждения и сетевое оборудование.

Оптимальная схема для каждой площадки в разных странах своя – она может включать различные источники энергии: и солнечные панели, и ветрогенераторы, и малые модульные реакторы. Однако даже самый надежный источник не сможет предотвратить сбой сервисов, если схема резервирования не гарантирует быстрое и автоматическое переключение на резерв (например, дизельные генераторы и ИБП).

Тренд к энергоэффективности в индустрии ЦОДов прослеживается четко, но без серьезной финансовой поддержки ни один дата-центр не сможет использовать возобновляемые источники энергии в качестве основного источника энергоснабжения. И не только потому, что это дорого, а потому, что ненадежно. Дата-центр, который отвечает за сохранность и доступность данных перед своими заказчиками, не может полагаться на погоду. Ни одно SLA не сможет обеспечить солнечную и ветреную погоду 365 дней в году, а значит, полагаться на природу в такой индустрии никак нельзя. Поэтому схема резервирования – более критический фактор для обеспечения надежной работы сервисов и минимизации возможных сбоев, нежели набор и типы используемых источников энергии. ИКС

Apple Park в Купертино, Калифорния

Источник: apple.com

Дата-центр Mount10 (The Swiss Fort Knox)

Лидерская позиция – это вызов, и мы его принимаем

В прошлом году «Парус электро» стала лидером в сегменте «ИБП» исследования «Карта вендоров для ЦОДов», проведенного iKS-Consulting. О локализации и комплектующих, тенденциях и реестре Минпромторга мы поговорили с учредителем компании Владимиром Хлебниковым.

– «Парус электро» давно работает на рынке систем бесперебойного питания. Как все начиналось? И почему «парус»?

– В первое слово названия мы вложили безграничность движения вперед, а второе говорит о направлении деятельности компании. Компания сразу сфокусировалась на важном и быстрорастущем рынке силовой электроники, начав с ИБП как самого массового и востребованного во всех отраслях продукта. Затем, накопив компетенции, мы освоили направление преобразователей для возобновляемой энергетики, рынок зарядных станций электромобилей и готовы развиваться дальше.

– Сегодня, когда на рынке пытаются работать много новых игроков, не все по понятным причинам готовы раскрывать, где и как осуществляются ключевые техпроцессы, НИОКР. Вам здесь скрывать нечего?

– Да, нам скрывать нечего: с момента создания мы инвестировали в развитие собственного конструкторского бюро, и сейчас наша команда выполняет все этапы – от разработки схемотехники, конструктивов, встроенного программного обеспечения до постановки изделия на серийное производство.

Для оптимизации стоимости изделий мы можем заказывать отдельные детали у специализированных отечественных производителей, но ключевые техпроцессы всегда оставляем за собой, чтобы гарантировать качество конечного продукта.

– Как у вас устроена логистика поставок? Склады оборудования, ЗИП? Как минимизируете «плечо» и время доставки до заказчика?

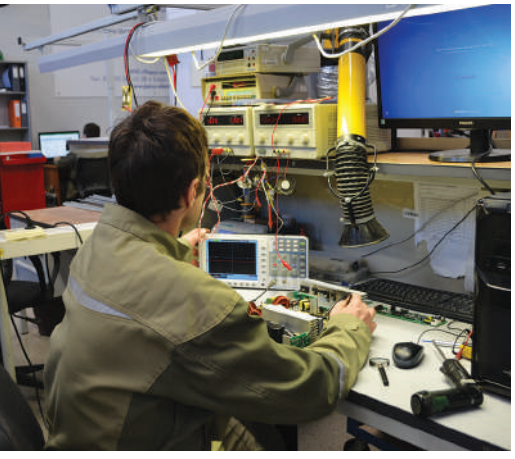
– В работе с заказчиками мы опираемся на наших дилеров – сейчас это более 130 компаний. С прошлого года наше логистическое плечо усилили крупнейшие российские дистрибьюторы, поддерживающие складские запасы однофазных «коробочных» ИБП мощностью 1–10 кВА.

Также на нашем складе постоянно в наличии основной модельный ряд однофазных и трехфазных ИБП и аккумуляторов к ним, вплоть до модульных ИБП мощностью 500 кВА. Таким образом обеспечивается стабильность и предсказуемость поставок. Для потребностей сервисной службы создан отдельный склад комплектующих и плат, что сокращает сроки ремонта и выезда на объекты.

– Насколько ваши ИБП по основным характеристикам соответствуют (а, может быть, превосходят) изделия мировых брендов, ушедших из России?

– При разработке своей линейки мы учли мировые тренды, преимущества и недостатки продукции конкурентов, поэтому с уверенностью можем сказать, что по техническим характеристикам и качеству не уступаем мировым производителям ИБП.

Например, сейчас наш модельный ряд включает ИБП с выходным коэффициентом мощности, равным 1,0, которые могут защищать больше современного оборудования с высокой активной мощностью. В трехфазных системах большой мощности применяем схему трехуровневого инвертора для повышения КПД и работы без перехода на батареи в расширенном диапазоне входных напряжений.



Мы делаем упор на развитие легко масштабируемых и отказоустойчивых модульных ИБП. Для крупных ЦОДов у нас есть решения на 100-кВт силовых модулях с уникальными на рынке показателями плотности мощности (т.е. мощности устройства в расчете на единицу занимаемой площади) – 600 кВт на 0,8 кв. м.

С крупными заказчиками мы практикуем совместное тестирование оборудования в заводских условиях, чтобы продемонстрировать его соответствие требованиям проектов.

– Традиционно отечественные ИБП строятся на импортных комплектующих, включая силовую электронику и контроллеры. Как вы видите перспективы разработки и производства этих комплектующих в России? Есть ли уже результаты?

– Для соответствия требованиям по импортозамещению ведем активную работу с отечественными производителями комплектующих и увеличиваем глубину локализации наших изделий. Мы выстроили процесс внедрения новых компонентов, который включает в себя проведение опытно-конструкторских работ, выпуск опытной партии и переход к серийному производству. Это позволяет исключить риск снижения качества конечного продукта при использовании новых комплектующих. Благодаря отлаженному процессу мы выполняем требования Минпромторга по глубине локализации и применению отечественной компонентной базы.

Конечно, в развитии компонентной базы у российской отрасли электроники впереди длинный путь, но мы прилагаем усилия, чтобы пройти его вместе с нашими поставщиками.

– Как «Парус электро» минимизирует риски импорта?

– Чтобы исключить зависимость от западных поставщиков, нам пришлось проделать определенную работу еще в 2022 г., и сейчас мы с уверенностью можем сказать, что не подвержены санкционным рискам.

Мы выстроили надежные цепочки поставки, а по ключевым компонентам всегда работаем с несколькими поставщиками, чтобы гарантировать непрерывность поставок.

– В каких мерах поддержки со стороны государства заинтересованы российские производители ИБП? Что эти меры могут дать развитию отрасли?

– В первую очередь нас волнует поддержка применения отечественной продукции в виде субсидий для заказчиков. Таким образом государство создаст стабильный спрос для российских производителей и поддержит развитие высокотехнологичного производства.

Что такое отечественный продукт для заказчика? Это не только выполнение задач импортозамещения, но и гарантия того, что производитель не уйдет с рынка и будет обеспечивать поддержку в течение всего жизненного цикла изделий. В последние полтора года мы видим огромный интерес к нам со стороны коммерческих заказчиков – они оценивают риски и издержки применения импортного оборудования в инфраструктуре и меняют свою политику в пользу отечественной продукции.

– Ваши трехфазные ИБП находятся в реестре Минпромторга, это важно для заказчиков. Насколько сложно было выполнить критерии включения в этот список?

– По сути, это результат 10-летней работы. Мы всегда делали акцент на корпоративном рынке и, когда ушли западные вендоры, оказались на технологическом фронтире среди российских компаний.

Процедура включения в реестр Минпромторга требует наличия полной конструкторской документации и отлаженного производства в России. Согласно правилам, для каждой модели следует подавать отдельную заявку и проходить процедуру верификации и инспекционного контроля. Сложный процесс, но мы научились с ним справляться.

– Какие тенденции на рынке систем бесперебойного питания ЦОДов вы можете отметить? Мировые? Российские?

– В мировом масштабе силовая преобразовательная техника, к которой относятся ИБП, растет примерно на 10–15% в год.

На российском рынке отмечу рост спроса именно на модульные конструктивы. Такие ИБП не только обеспечивают высокую отказоустойчивость благодаря резервированию основных узлов, но позволяют легко масштабировать систему путем добавления модулей. Можно планировать инвестиции в развитие инфраструктуры по мере роста потребностей предприятия.

Для высоконагруженных объектов огромное значение имеет плотность мощности, а также повышенный КПД для увеличения энергоэффективности.

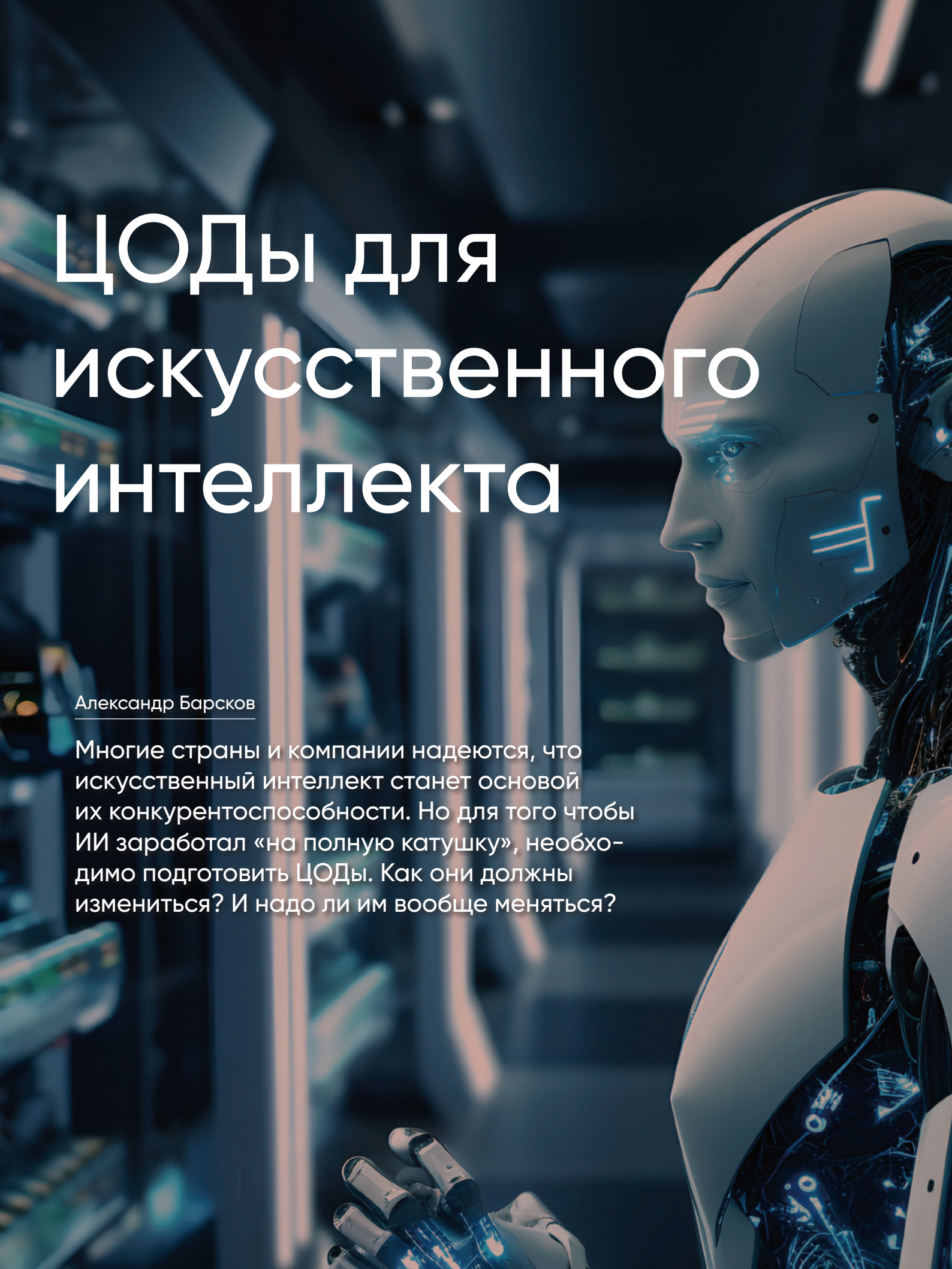
И, конечно, применение литиевых батарей наравне с традиционными свинцово-кислотными аккумуляторами. Уже сейчас наши системы поддерживают литиевые батарейные кабинеты на основе технологий LFP и NMC, а также работают с накопителями на суперконденсаторах.

– Каковы ваши дальнейшие планы? Ведь лидерство часто сложнее удержать, чем завоевать.

– Лидерская позиция – это хороший вызов, и мы принимаем его в новом году. В наших планах – развивать модельный ряд, дополнительные сервисы и услуги, чтобы оставаться номером один на рынке ИБП.

Для нас ЦОДы – приоритетная отрасль, в которой заключен огромный потенциал. Как в начале 20-го века электрификация была основой для индустриализации, так сейчас дата-центры станут основой новой экономики данных.

ЦОДы для искусственного интеллекта



Александр Барсков

Многие страны и компании надеются, что искусственный интеллект станет основой их конкурентоспособности. Но для того чтобы ИИ заработал «на полную катушку», необходимо подготовить ЦОДы. Как они должны измениться? И надо ли им вообще меняться?

В последнее время много рассуждают о том, как искусственный интеллект изменит процессы эксплуатации ЦОДов. Безусловно, системы с использованием ИИ способны существенно повысить уровень автоматизации и эффективность многих важных процессов, включая выделение и конфигурирование различных ресурсов (электропитание, охлаждение, технологическое пространство), управление инженерными системами, рабочей (ИТ-) нагрузкой, обеспечение физической и информационной безопасности (рис. 1).

Однако прежде чем обсуждать то, как ИИ в перспективе изменит процессы эксплуатации ЦОДов, важно разобраться, как сами ЦОДы должны измениться, чтобы обеспечить эффективную работу систем ИИ. Ведь дата-центр – это не только потребитель результатов деятельности ИИ, но и платформа для функционирования соответствующих приложений. А они представляют собой во многом нетипичную рабочую нагрузку.

Системы с ИИ требуют огромных объемов вычислительных ресурсов, особенно на стадии обучения моделей. Для повышения производительности таких систем предпочтительно использовать невиртуализированные среды, а именно серверы с графическими процессорами (GPU).

Bare metal рулит

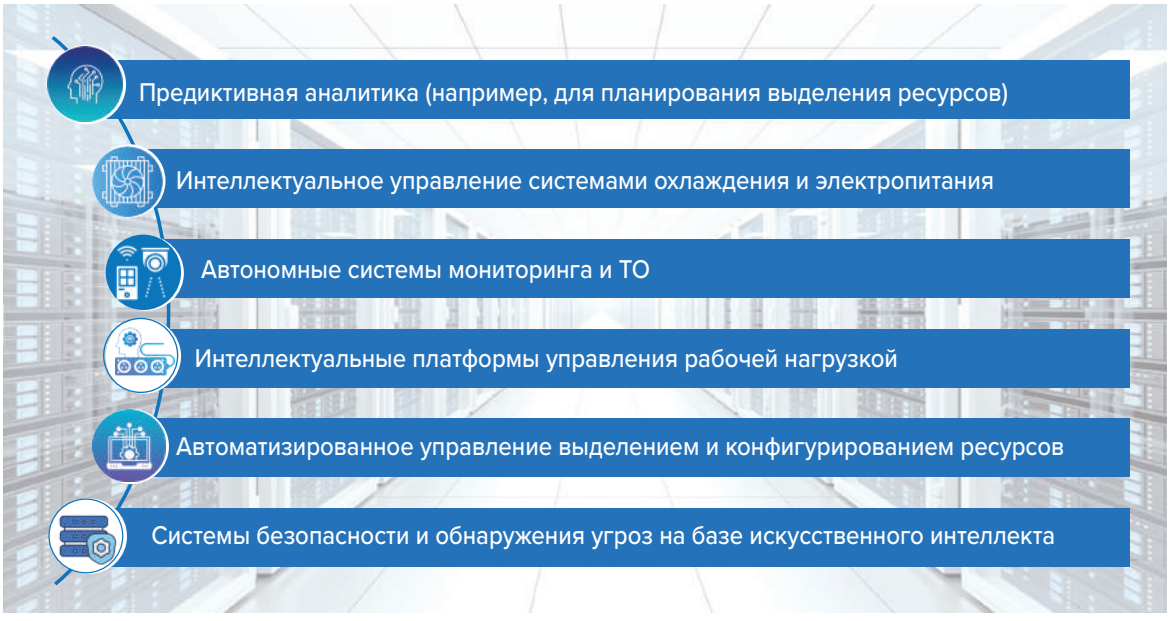
Последние годы виртуализация ИТ-инфраструктуры была в числе главных трендов. Причина понятна: виртуализация позволяет более эффективно использовать физические ресурсы, она делает инфраструктуру более гибкой и адаптивной. Неудивительно, что именно виртуальные машины стали основным инфраструктурным ресурсом для размещения рабочих ИТ-нагрузок. Но с учетом «любви» искусственного интеллекта к «голому железу» операторам ЦОДов для поддержки соответствующих приложений придется расширять предложение сервисов bare metal.

Запуск рабочих нагрузок на «голом железе» существенно облегчает жизнь сервис-провайдеру: не нужны никакие гипервизоры, оркестраторы и другие элементы платформ виртуализации. Но при этом может понадобиться обновить серверный парк, а возможно, и стойки, в которых размещается ИТ-оборудование. Провайдеры нередко практиковали приобретение мощных серверов, которые затем разделялись на множество виртуальных машин. Но в ситуации, когда потребуется много отдельных физических серверов, ориентация на мощные компьютеры может оказаться неоправданной. Логичнее установить большее количество менее мощных серверов с GPU-ускорителями. Короче говоря, предстоит масштабная замена серверного парка.

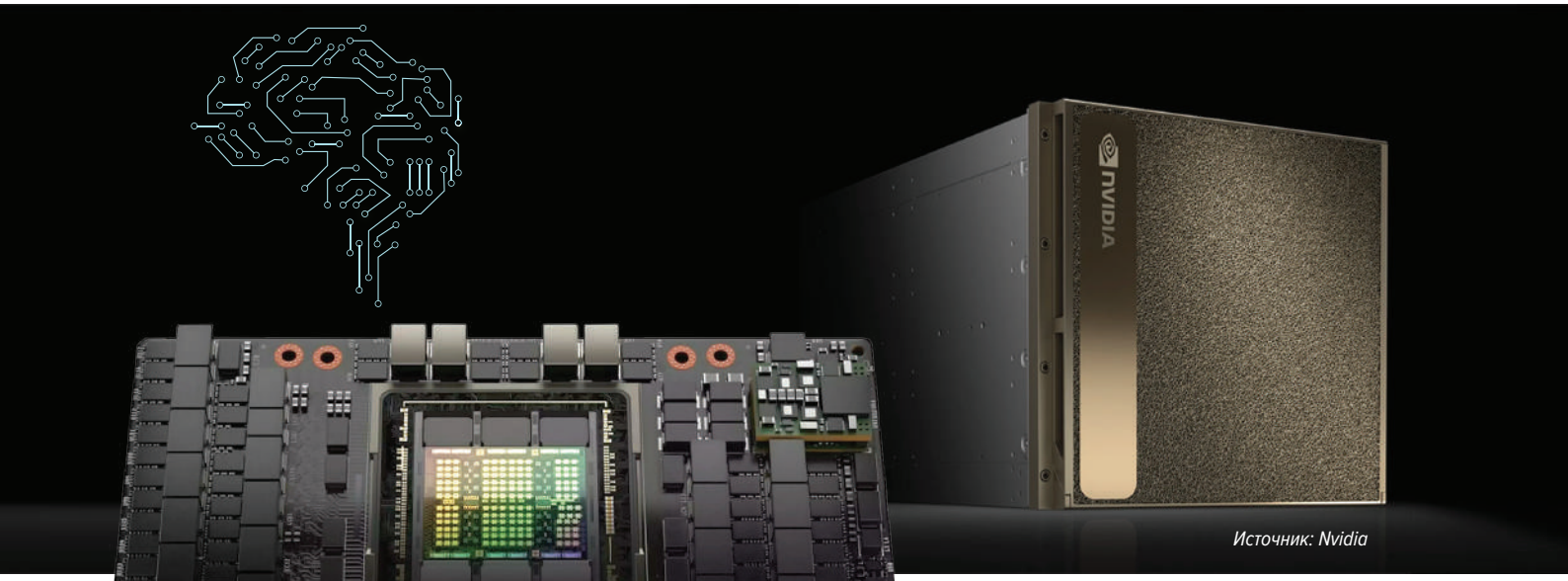
Низкая задержка – высокая плотность

Системам с ИИ нужны каналы связи со сверхнизкой задержкой. Следует заметить, что ЦОДы всегда стремились иметь высокопроизводительные сети с минимальной задержкой. Для снижения задержки в свое время классическая трехуровневая сетевая архитектура «доступ – агрегация – ядро» была заменена на архитектуру leaf – spine, уменьшающую число сетевых пролетов (а значит, и задержку) между узлами. Ну а каналы передачи данных в современных дата-центрах уже вышли на уровень 100G и выше. Чтобы в полной мере воспользоваться преимуществами искусственного интеллекта, необходимо еще больше снизить задержку. Здесь уже на первое место выходит вопрос расстояния, а потому системы для ИИ размещают максимально компактно, что увеличивает плотность энергопотребления.

С учетом «любви» ИИ к «голому железу» операторам ЦОДов придется расширять предложение сервисов bare metal



◀ Рис. 1. Примеры использования ИИ в ЦОДах



Источник: Nvidia

▲ **Рис. 2.** **Nvidia H100 GPU на модуле SXM5**

▶ **Рис. 3.** **Сервер Nvidia DGX**

Чтобы разобраться, насколько плотной должна быть среда для ИИ, давайте углубимся в «анатомию» ИТ-систем для искусственного интеллекта. Флагманский процессор для таких систем – Nvidia H100 (рис. 2), выпущенный компанией в 2022 г. под кодовым названием Hopper (в честь ученого-компьютерщика ВМС США Грейс Хоппер, которая стала пионером компьютерного программирования). Этот чип изготавливается тайваньской TSMC по 4-нм техпроцессу, что обеспечивает примерно на 50% большее количество транзисторов (около 80 млрд) по сравнению с предыдущим семейством чипов Ampere.

К концу 2023 г. Nvidia поставила, по разным оценкам, 500–600 тыс. чипов Hopper. В текущем году будет выпущено уже 1,5–2 млн этих чипов, и серверами с ними будет полностью заполнено примерно 50 тыс. ИТ-стоек (здесь и далее в расчетах предполагается использование наиболее популярных на сегодня стоек высотой 42U). Однако, скорее всего, стоек будет гораздо больше из-за ограничений, связанных с доступными плотностью электрической мощности и производительностью систем охлаждения.

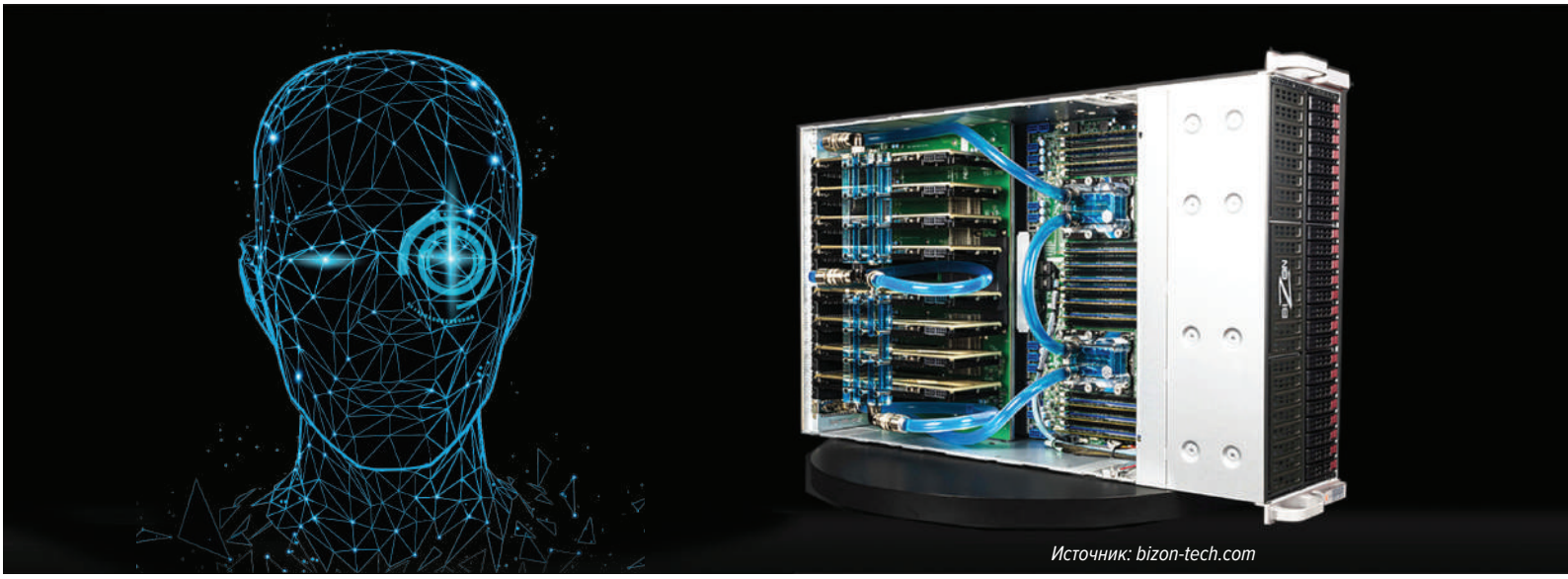
Если бы все эти системы искусственного интеллекта были постоянно полностью загружены, это означало бы добавление около 2000 МВт новой ИТ-нагрузки. Важно заметить, что эта оценка проведена только для чипов Hopper, тогда как у той же Nvidia немало других моделей GPU. Есть и другие поставщики графических процессоров.

Но вернемся к вопросу плотности. Одна из наиболее популярных систем для ИИ-приложений – серверы Nvidia DGX. Сегодня доступно уже четвертое поколение таких машин. Сервер DGX H100 (рис. 3) имеет восемь графических процессоров GPU H100, два CPU Intel Xeon Sapphire Rapids, 8 × 400 Гбит/с InfiniBand/Ethernet-коммутатор ConnectX-7, а также высокоскоростное хранилище NVMe SSD на 30 Тбайт. Этот сервер имеет высоту 8U и номинальную мощность 10,2 кВт, т.е. 1,275 кВт на 1U. Типовое потребление (и, соответственно, тепловыделение), вероятно, ближе к 7–8 кВт. Nvidia предлагает инструменты управления питанием, чтобы клиенты могли размещать до четырех систем в стойке, не нарушая ограничений по подаче электроэнергии.

Даже при максимально плотной набивке стойки серверами DGX H100 ее максимальная мощность составит 35 кВт (для расчета взято среднее энергопотребление одного сервера 7 кВт). При этом некоторые ИТ-визионеры пугают нас тем, что для ИИ нужны стойки на 50 кВт и выше. Практики же говорят, что реальная плотность на самом деле еще ниже. Так, по словам представителей компании Selectel, их платформа AI&ML (искусственного интеллекта и машинного обучения) функционирует на стойках мощностью 12–15 кВт.

Если принять за верхний уровень 35 кВт на стойку, то это тепловыделение при известных ухищрениях, таких как качественная изоляция воздушных потоков, установка внутрирядных кондиционеров и пр., вполне можно снять с помощью апробированных годами систем воздушного охлаждения. В России есть ЦОДы, в которых, по заявлениям их руководителей, воздухом может сниматься до 50–55 кВт на стойку. Но эти решения пока нельзя отнести к типовым.

Использование перспективных систем жидкостного охлаждения для серверов ИИ (рис. 4) интересно тем, что позволит снизить энергопо-


Источник: bizon-tech.com

▲ **Рис. 4. Сервер с GPU Nvidia и жидкостным охлаждением**

требление за счет отказа от вентиляторов (они могут потреблять до 20% всей мощности) и максимально увеличить производительность GPU и CPU. Непосредственное охлаждение жидкостью дает возможность снимать до 100 кВт (и даже более) тепловой нагрузки с одной стойки или сопоставимой с ней по размерам ванны (куда погружаются платы серверов).

Однако системы жидкостного охлаждения пока не получили широкого распространения. Основная причина – отсутствие стандартов для этой технологии. Разные производители используют разные охлаждающие жидкости, нестандартизованные блоки распределения жидкости, а потому ЦОДы могут оказаться привязаны к одному производителю подобной системы охлаждения. В свою очередь, вендоры ИТ-оборудования не обеспечивают такой же полной поддержки систем жидкостного охлаждения, как воздушного. Наконец, для работы с системами жидкостного охлаждения нужна переподготовка персонала, а это требует времени и денег. Но даже при обученном персонале внедрение таких систем повышает эксплуатационные риски из-за относительно низкой зрелости процедур и может привести к более высокому, чем обычно, числу сбоев и неполадок.

Всегда ли нужны GPU

Но всегда ли системам ИИ нужны большие ресурсы GPU? На самом деле они требуются на этапе обучения модели. Затем потребность в ресурсах заметно снижается – до тех пор, пока не придет время переобучать модель. Поэтому оснащать корпоративный ЦОД дорогостоящими серверами с GPU, чтобы использовать их на полную мощность только эпизодически, вряд ли разумно.

Рост популярности приложений с ИИ станет очередным мощным катализатором перехода на сервисную модель, в рамках которой клиенты смогут получать доступ к необходимым ресурсам, размещенным в коммерческом ЦОДе, и соответственно оплачивать только реально потребленные ресурсы. Неудивительно, что аналитики прогнозируют бум спроса на услуги типа GPUaaS. Так, по предварительным данным Future Market Insights, глобальный рынок услуг GPUaaS в 2023 г. составил около $3,9 млрд. В ближайшие 10 лет его объем будет ежегодно расти в среднем на 40,8% и к 2033 г. достигнет $119,6 млрд.

Революция, связанная с искусственным интеллектом, еще не завершена. Поэтому нельзя точно предсказать, как искусственный интеллект изменит инфраструктуру и работу ЦОДов. Ведь в более отдаленной перспективе в процесс могут вмешаться квантовые компьютеры со своими специфическими требованиями к системам электропитания и охлаждения. Но можно с уверенностью утверждать, что такие изменения, как увеличение числа серверов с поддержкой GPU и более гибкие модели их использования, окажутся критичными в мире, ориентированном на искусственный интеллект. Операторы ЦОДов, которые хотят получить свой кусок пирога на рынке ИИ, должны оперативно обновить инфраструктуру, чтобы она соответствовала специфическим требованиям соответствующих приложений.

По прогнозу Nvidia, уже в ближайшее время на модернизацию центров обработки данных для ИИ будет потрачено около $1 трлн. Поэтому, чтобы хорошо заработать на ИИ, провайдерам надо сначала потратиться на подготовку своих дата-центров. ИКС

Cloud X: какими должны быть облака

Облачный регион на базе собственных гипермасштабируемых ЦОДов с нулевым углеродным следом, edge-ЦОДы и ПО исключительно собственной разработки… О направлениях и приоритетах деятельности компании Cloud X – ее генеральный директор Денис Хлебородов.

– Компания Cloud X пока мало известна на российском рынке. Расскажите об истории ее создания, основных направлениях работы.

– Компания Cloud X создана 1 октября 2021 г. и является частью холдинга En+ Group. Основная сфера нашей деятельности – предоставление услуг облачных вычислений по моделям IaaS, PaaS и SaaS. Выделение данного направления внутри холдинга имело две основные цели. Первая – это повышение темпов и качества цифровой трансформации всех компаний холдинга. Второе – это поддержка инициатив Правительства России по стратегическому развитию цифровой экономики.

Холдинг En+ всегда активно инвестировал в инновации, но эти инновации были связаны главным образом с отраслями энергетики и металлургии. Если цифровую трансформацию компаний можно до некоторой степени провести, не меняя принципиально модель использования ИТ на предприятиях, то в цифровой экономике существуют проблемы, которые нельзя преодолеть без применения публичных облаков, в частности, без создания среды для формирования API-экономики, экономики данных и работы сквозных процессов машинного обучения. Качество последних напрямую влияет на скорость внедрения ИИ во все сферы человеческой деятельности. Для охвата решений во всех этих направлениях возникла идея создать публичное облако Cloud X.

Бизнес инвестиционной группы En+ имеет высокую степень диверсификации. Ее предприятия занимают лидирующие позиции во множестве отраслей: энергетике, металлургии, машиностроении, финансовом секторе, сельском хозяйстве, строительстве, аэропортовом, логистическом, отельном бизнесах и др. По мере облачной трансформации предприятий успешный отраслевой опыт будет отражаться в портфеле наших вертикальных решений. В итоге мы должны будем прийти к модели BaaS (Business as a Service), в рамках которой создание любого предприятия в физическом смысле представляет собой установку набора, условно говоря, исполнительных механизмов, пусть даже сложных, а вся остальная часть вместе с описанием задается кодом.

Компания Cloud X пока не слишком известна, поскольку на первом этапе мы решили сосредоточиться на разработке и тестировании, сделав приоритетом не достижения в области маркетинга и рекламы, а качество наших продуктов. Помимо программной разработки компания сегодня также занимается проектированием и строительством ЦОДов, которые будут составлять глобальную инфраструктуру для облачной платформы и продуктов.

– В чем конкурентные преимущества компании на российском облачном рынке?

– В первую очередь я бы отметил наш подход к организации глобальной инфраструктуры. Мы заложили в нее три модели для того, чтобы охватить различные сценарии потребления: во-первых, это облачные регионы, состоящие из удаленных друг от друга на расстояние до 40 км трех гипермасштабируемых дата-центров мощностью до 150 МВт каждый; во-вторых, инфраструктура граничных вычислений и, в-третьих, инфраструктура для размещения на территории клиента, в том числе в закрытых сегментах критической информационной инфраструктуры без нарушения требований инфобезопасности. Создание облачного региона в Сибири даст возможность снизить риски стратегической безопасности с учетом военных угроз.

Конфигурация наших машинных залов позволяет размещать не только серверы для высокоплотных облачных вычислений, но и суперкомпьютеры. Для узлов суперкомпьютеров мы можем предложить кабинеты, поддерживающие мощность 25 или даже 32 кВт. Еще одно наше преимущество – приверженность целям устойчивого развития. Облачные регионы Cloud X имеют нулевой углеродный след благодаря использованию для энергоснабжения ЦОДов гидроэнергетического потенциала En+.

Другое преимущество заключается в том, что все ПО Cloud X либо написано с нуля внутри компании, либо базируется на программных продуктах с открытым исходным кодом. Последнее существенно ускоряет разработку, хотя, конечно, требует устранения присущих такому ПО недостатков – отсутствия тех или иных функций, неоптимальности стека, низкой производительности, не замеченных сообществом уязвимостей и ошибок. Мы разделяем наше ПО на группы по источникам потоков требований: на компоненты облачной платформы, продукты облака, предоставляемые по моделям IaaS и PaaS, и самостоятельные дистрибутивы, которые могут использоваться без облака и ПО и проходят сертификацию в системе сертификации ФСТЭК России.

Конкурентным преимуществом облачной платформы Cloud X является и то, что она основана на платформе управления ресурсами собственной разработки, которая выстраивает абстракцию над всеми ресурсами и продуктами облака. В платформе применяется многоуровневая ресурсная модель. Выбранный архитектурный принцип позволяет учитывать высокую динамику развития компонентов и абстрагировать их друг от друга. Важный слой платформы – программно определяемые сети, которые позволяют обеспечить «склейку» сетей платформ виртуализации, выстроив клиентские сети. Есть множество других технических аспектов, которые обеспечивают удобство для клиентов и делают их работу близкой к тому, что можно получить в таких облаках, как Azure, GCP или AWS.

– Каковы ваши планы развития сети ЦОДов? Как обеспечивается их связность, доступность и отказоустойчивость?

– ЦОДы уровня региона разворачиваются в Сибири в г. Усть-Илимске. (Есть планы создать регион в Республике Карелия, но они пока поставлены на паузу.) В Усть-Илимске уже определены земельные участки, получены техусловия. Проектирование первого ЦОДа завершено, мы находимся в процессе получения разрешения на строительство. На втором участке идут инженерные изыскания и проектно-изыскательские работы.

Среди требований к инфраструктуре ЦОДов на первый план выходит их географическая близость к клиентской части и уже на второй – вопросы масштабируемости, энергоэффективности и даже надежности. Поэтому для edge-ЦОДов Cloud X применяются две модели. Первая – партнерская модель, предполагающая использование существующей на рынке инфраструктуры по модели colocation. Она касается операторов ЦОДов и операторов связи – 4G/5G, LPWAN. Вторая – создание собственных edge-ЦОДов. Причем сначала выбираются точки, где будут строиться такие ЦОДы, определяются возможные условия их размещения, затем ищется оптимальное технико-экономическое решение с учетом существующей операционной модели.

Каждый регион Cloud X будет образован как минимум тремя ЦОДами – для уменьшения возможных потерь в случае аварии в одном из них. Для организации связи между ЦОДами в пределах одного облачного региона планируется построить собственную волоконно-оптическую сеть Cloud X. Физическая топология опорной транспортной сети – кольцо. Логическая топология – полносвязное взаимодействие между всеми ЦОДами. Проектная пропускная способность данной сети – множество каналов связи 400 Гбит/с со спектральным уплотнением DWDM, внешние каналы связи – множество каналов по 100 Гбит/с. Безопасность каналов связи в пределах региона планируется обеспечивать криптографическими методами на уровне транспондеров DWDM. Распределение ключей предполагается осуществлять посредством квантовой криптографической системы выработки и распределения ключей. Резервирование вычислительных подсистем достигается за счет построения геораспределенных вычислительных кластеров. Задержки при передаче данных между ЦОДами не превышают 2 мс, общая длина кабеля оптического волокна не более 50 км.

Помимо высокоскоростных оптических интерконнектов между ЦОДами одного облачного региона планируется организовать сегмент собственной транспортной сети Cloud X для взаимодействия между облачными регионами и подключения каждого ЦОДа ко всем операторам связи, имеющим собственные сети передачи данных с точками присутствия в регионе. На транспортной сети организуются узлы межрегионального обмена (MPO, Inter-Region Exchange, IRX), которые обеспечивают подключение к внешним каналам связи (интернет, MPLS VPN).

Клиенты будут подключаться к сервисам Cloud X либо через интернет, либо по выделенным каналам связи. В качестве альтернативного способа подключения предлагается концепция граничных (edge-) узлов, которые размещаются в городах присутствия клиентов. Эта концепция предполагает организацию магистральных каналов связи между точками MPO и граничными узлами. Таким образом обеспечиваются простота и гибкость подключения клиентов к сервисам, размещенным в облаке, снижается стоимость подключения. Узлы транспортной сети соединяются между собой по принципу «каждый с каждым». Инфраструктура транспортной сети поддерживает подключение рабочей нагрузки через порты 400 Гбит/с.

В настоящее время мы создали в Москве площадку, которая является уменьшенной копией одного облачного региона, и проводим на ней все виды тестов нашей платформы.

– Чем хороши граничные вычисления?

– Граничные вычисления имеют несколько важных преимуществ. Во-первых, чувствительные к времени отклика взаимодействия могут обрабатываться промежуточным сервисом, который располагается в непосредственной географической близости к клиенту. Во-вторых, они позволяют оптимизировать затраты на каналы передачи данных. Это достигается за счет предварительной обработки потока данных и последующей отправки результатов обработки в облачный регион, за счет сокращения затрат на каналы связи при взаимодействии с облаком – благодаря совместному использованию транспортной сети, кешированию и буферизации данных. Роль такого типа вычислений чрезвычайно важна, они обеспечивают бесшовность работы при взаимодействии с чувствительными к задержкам источниками либо с источниками большого объема «быстрых» данных. Возможность такой балансировки вычислений и данных нужна огромному количеству приложений.

– Где будут первые edge-ЦОДы?

– Мы проектируем два edge-ЦОДа – один в Нижнем Новгороде, второй – в Москве. В настоящее время ведем переговоры с некоторыми владельцами ЦОДов, мощности которых рассматриваются в качестве инфраструктуры граничных вычислений для Cloud X.

Анализ отказов в ЦОДах

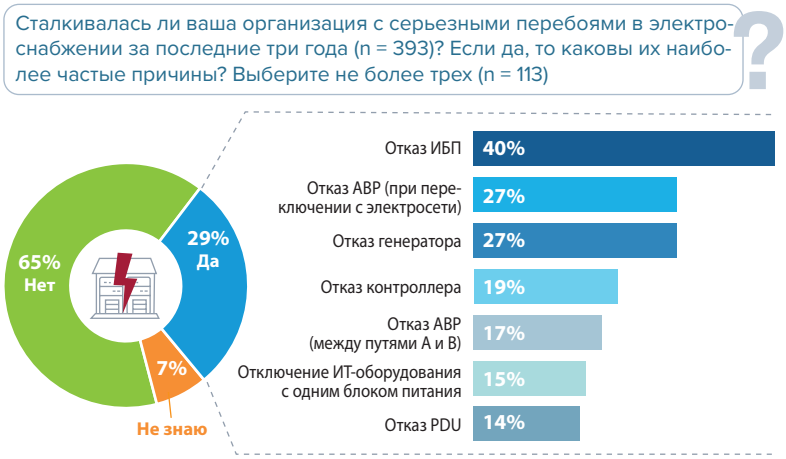
Окончание. Начало см. в «ИКС» № 4'2023, с. 52.
Печатается с разрешения Uptime Institute

Энди Лоуренс, исполнительный директор по исследованиям, **Ленни Саймон**, старший научный сотрудник, Uptime Institute

Отказы в ЦОДах обусловлены в основном проблемами в системах электроснабжения и сетевой инфраструктуре, ошибками в ПО, а также человеческим фактором. Рецепты предупреждения: повышение уровня отказоустойчивости и резервирования, эффективности эксплуатации и компетентности персонала.

Отказы из-за систем электроснабжения

Как говорилось в первой части этой статьи, проблемы с электроснабжением – главная причина отказов на большинстве объектов. Инциденты, связанные с отключением электропитания, обычно случаются внезапно, могут распространяться на всю площадку и оказывать серьезное влияние на предоставление услуг. Хотя диагностика проблемы и восстановление электропитания обычно выполняются достаточно быстро, перезагрузка ИТ-систем и полная синхронизация баз данных могут занять много часов. Поломка же оборудования в результате такого инцидента способна привести к тому, что ЦОД еще долго не сможет оказывать услуги в соответствии с SLA – пока отказавшее оборудование не будет заменено.



Источник: Uptime Institute Data Center Resiliency Survey, 2023

▲ **Рис. 1. Основные причины отказов в системе электропитания**

В исследовании отказоустойчивости ЦОДов (2023 г.) о том, что за последние три года на их объектах произошли серьезные сбои, вызванные проблемами с электроснабжением, сообщили примерно треть операторов. Причем по сравнению с предыдущим годом картина изменилась незначительно. Основная причина отключения электричества – сбой в работе ИБП (рис. 1). С отказами генераторов и АВР столкнулись чуть более четверти операторов.

Для выхода из строя статических ИБП есть несколько причин:

- Поломка вентиляторов, которые постоянно находятся в работе, из-за их низкого качества. Отказ одного вентилятора не приводит к выходу устройства из строя, но когда ломаются несколько, ИБП остановится.
- Выход из строя демпфирующих конденсаторов из-за износа. Регулярное профилактическое обслуживание сократит количество отказов.
- Выход из строя АКБ. Они требуют тщательного мониторинга и соблюдения графика замены. Батареи часто выходят из строя именно из-за недочетов в обслуживании.
- Сбой в работе инверторного блока. Эта причина встречается реже и обычно возникает при перегрузке устройства, хотя износ также может привести к отказу.

Неполадки в ИБП более вероятны при длительном сроке службы, поэтому проблемы с цепочкой поставок/заменой могут привести к увеличению числа сбоев. Операторы ЦОДов, не имеющие возможности отключать любой элемент

оборудования для технического обслуживания без прерывания сервисов, с большей вероятностью отложат техобслуживание или замену.

Генераторы надежны, но требуют регулярного техобслуживания, проверок топлива и тестирования. Блоки АВР, как правило, надежны, но в них могут возникать сбои на уровне контроллеров, например при нарушении их электропитания. Менее распространены неисправности, вызванные механическими неполадками, такими как износ подшипников или заклинивание переключателя.

Отказы в сетевой инфраструктуре

В последние годы сетевые неполадки все чаще приводят к отказам в работе ИТ-систем. Исследование отказоустойчивости ЦОДов (2023 г.) показало (рис. 2), что двумя наиболее распространенными причинами перебоев в работе сети и/или обеспечении коннективности являются сбои в управлении конфигурацией/изменениями (45% респондентов) и сбои в работе сторонних сетевых провайдеров (39%), и эти цифры схожи с данными предыдущих лет.

Ни одна из двух этих причин не вызывает удивления. В прежние времена сетевое взаимодействие было гораздо более статичным, изначально настроенные маршрутизаторы и коммутаторы никто без нужды не трогал. Но современные сети с динамической коммутацией и программно определяемыми параметрами постоянно оптимизируются и реконфигурируются. Ошибки неизбежны, и в сложной сетевой среде с высокой пропускной способностью частые мелкие ошибки могут распространяться, приводя к каскадным сбоям, которые бывает трудно остановить, диагностировать и устранить.

Сети сложны не только с технической точки зрения, но и с точки зрения эксплуатации. В то время как корпоративные ЦОДы могут обслуживаться только одним или двумя телеком-провайдерами, в крупных кампусах коммерческих ЦОДов, предоставляющих услуги colocation, присутствует много операторов связи. Некоторые из них могут совместно использовать кабели или оборудование связи, что создает общие точки потенциального отказа или ограничения пропускной способности. Схемы ответственности и отчетность также могут быть сложными. Неудивительно, что 39% респондентов, участвовавших в опросе, за последние три года сталкивались с перебоями, вызванными проблемами в сетях сторонних провайдеров, которые они не контролировали.

Большинство из тех, кто избежал простоев, связанных с сетью, объясняют это принятием таких мер, как обеспечение избыточности и повышение отказоустойчивости сети.

Отказы, связанные с ИТ-системами/ПО

За последние три года более трети операторов столкнулись с серьезными перебоями в работе своих объектов, вызванными системными или программными неполадками (рис. 3). Как и в случае с сетевой инфраструктурой, сбои в работе ИТ-систем/ПО обусловлены сложностью и масштабом современных ИТ-комплексов, а также растущей ролью ПО в обеспечении доступности ИТ-сервисов в распределенных сетях. Проблемы с синхронизацией баз данных, балансировкой нагрузки и управлением трафиком могут привести к частичной или полной остановке ИТ-сервисов, запущенных более чем в одном ЦОДе или в одной зоне доступности.

Программные сбои в основном вызваны изменениями конфигурации, обновлениями, патчами и пр., которые приводят к нестабильности и

Сталкивалась ли ваша организация с серьезными перебоями в работе, вызванными проблемами с сетью/коннективностью, за последние три года (n = 406)? Если да, то каковы их наиболее частые причины? Выберите не более трех (n = 174)

Источник: Uptime Institute Data Center Resiliency Survey, 2023

▲ **Рис. 2. Основные причины отказов, связанных с сетью**

Сталкивалась ли за последние три года ваша организация с серьезными отказами, вызванными сбоем в работе ИТ-систем/ПО (n = 385)? Если да, то каковы их наиболее частые причины? Выберите не более трех (n = 136)

Источник: Uptime Institute Data Center Resiliency Survey, 2023

▲ **Рис. 3. Основные причины серьезных сбоев в работе ИТ-систем/ПО**

Источник: Uptime Institute Data Center Resiliency Survey, 2023

▲ Рис. 4. Наиболее распространенные причины отказов, связанных с человеческим фактором

непредвиденным ошибкам. Если они распространяются по сетям, локализовать проблему труднее. Примерно каждая десятая организация заявила, что отказы были вызваны кибератаками, например программами-вымогателями и DDoS-атаками. Это меньше, чем в предыдущие годы, однако когда такие инциденты случаются, они могут быть чрезвычайно серьезными и дорогостоящими.

Каковы бы ни были причины отказов, основными методами их предотвращения всегда называют отказоустойчивость и резервирование. Это не удивительно и подтверждает обоснованность многолетних масштабных инвестиций в ЦОДы и совершенствование архитектур критически важных объектов. Повышение эффективности процессов эксплуатации и управления, а также компетентности персонала – также распространенное средство предотвращения отказов.

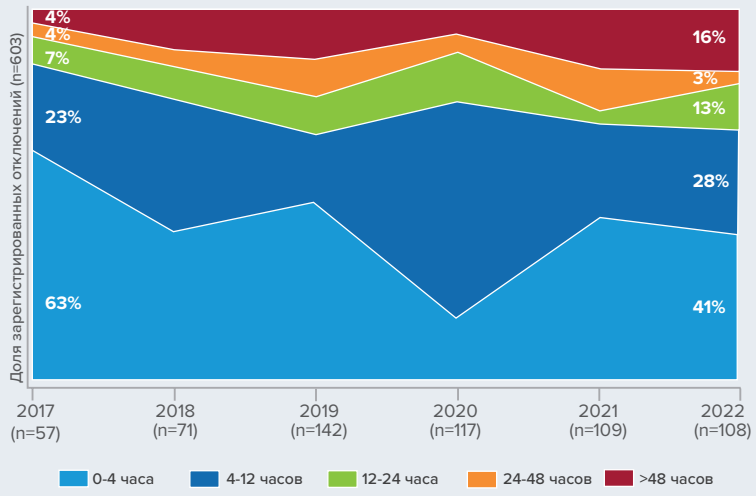
Ошибки, связанные с человеческим факторов

Эксперты Uptime Institute считают, что человеческие ошибки следует рассматривать отдельно от других причин отказов. Это очень важный фактор, но редко он является единственной причиной или первопричиной. По данным Uptime, собираемым более 25 лет, человеческая ошибка так или иначе имела место в большей части отказов – от 2/3 до 4/5 всех инцидентов.

Анализировать человеческие ошибки операторам ЦОДов всегда было сложно. Сбой может

Публичные аварии: продолжительность и примеры

Чем дольше длится отключение, тем больше вероятность того, что его последствия будут дорогостоящими и разрушительными и оно привлечет внимание СМИ. Данные по публичным авариям показывают, что последствия большинства (70%) громких инцидентов устраняются в течение 12 ч, а многих гораздо быстрее. Однако начиная с 2019 г. (данные до этого года менее надежны) наблюдается тревожная тенденция: растет число отключений, полноценное восстановление после которых не удалось завершить даже через 48 ч.



Перебои в работе, причина которых не была известна, исключены из анализа.
Указано время восстановления сервиса, а не полного восстановления бизнес-процессов.

Источник: Uptime Institute Intelligence, 2023

Причин этого может быть несколько: например, серьезные пожары и сложности синхронизации распределенных данных и систем управления. Очевидно и то, что масштабные атаки программ-вымогателей, которые обычно требуют отключения всех потенциально уязвимых систем, случаются все чаще.

В последнее время каждый год происходит примерно 15–20 отказов, которые по классификации Uptime относятся к серьезным и тяжелым (категории 4 и 5), т.е. могут привести к высоким финансовым потерям, ущербу репутации, угрозам жизни или безопасности и существенным нарушениям нормативных правил.

Крупнейшие отказы, о которых публично сообщалось в 2022-м и начале 2023 гг. (см. таблицу), затронули в основном компании, предоставляющие телекоммуникационные, облачные и/или цифровые услуги, т.е. сектора, в которых перебои в работе ИТ-систем отразятся на многих пользователях. Государственный сектор и здравоохранение также весьма чувствительны к отказам ИТ-систем.

быть связан с недочетами в организации процесса эксплуатации, с усталостью персонала, недостаточной его обученностью или обеспеченностью ресурсами, а также с тем, что само оборудование оказалось неоправданно сложным в эксплуатации. Такие факторы, как усталость, в конечном счете могут быть обусловлены дефицитом персонала или длинными сменами.

Классифицировать причины отказов также нелегко. Например, если оборудование выходит из строя из-за ошибки в ПО, допущенной на заводе, следует ли относить ее к человеческому фактору? Человеческая ошибка часто может играть определенную роль и в перебоях в работе, которые объясняются другими причинами.

В наших недавних исследованиях по отказоустойчивости мы пытались понять причины некоторых отказов, связанных с человеческими ошибками. Такие отказы в основном вызваны либо несоблюдением персоналом процедур (даже в тех случаях, когда они согласованы и кодифицированы), либо недостатками самих процедур (рис. 4).

В ходе глобальных ежегодных опросов, проводившихся с 2019 по 2022 гг., подавляющее большинство менеджеров и операторов ЦОДов заявили, что их недавние наиболее значимые отключения можно было бы предотвратить при улучшении управления и процессов эксплуатации (рис. 5).

Источник: Uptime Institute Global Survey of IT and Data Center Managers, 2022

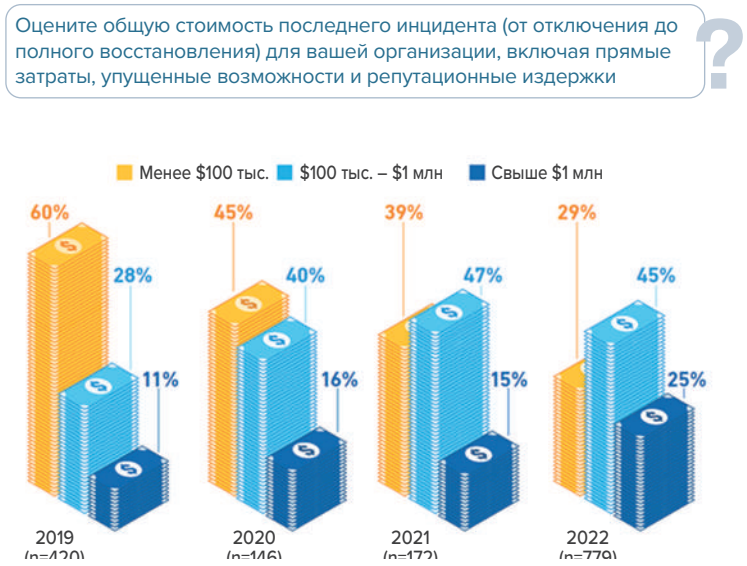
◀ Рис. 5. Большинство операторов считают, что отказ можно было предотвратить

Приведенные цифры подчеркивают важность рекомендации, которую эксперты Uptime всегда дают владельцам и операторам ЦОДов: хорошее обучение и хорошо продуманные и отрепетированные процессы эксплуатации играют ключевую роль в сокращении числа простоев, причем все эти меры можно реализовать без больших затрат.

Восемь крупнейших отказов в 2022-м и начале 2023 гг.

Компания/ организация	Категория	Год (квартал)	Причина	Последствия
Федеральное управление гражданской авиации (США)	5	2023 (I)	Конфигурация ПО / ошибка в БД	Запрет на вылет всех рейсов в США. Тысячи рейсов были отменены или задержаны
Kakao (Южная Корея)	5	2022 (IV)	Пожар в батарейной комнате	Большинство пользователей в Южной Корее сталкивались с отказом в обслуживании в течение 8 ч. CEO был уволен. Правительство инициировало специальное расследование. Множество судебных разбирательств
KDDI (Япония)	5	2022 (III)	Сетевая инфраструктура / ошибка в конфигурации	39 млн пользователей получали отказ в обслуживании в течение 86 ч. Были затронуты критические сервисы в разных отраслях
Google (глобально)	4	2022 (III)	Проблема при обновлении ПО	Поисковик Google и использующие его приложения (в частности, Google Maps и Google Images) в течение 40 мин по всему миру находились в режиме офлайн или их работа существенно замедлилась
CommonSpirit Health (США)	4	2022 (IV)	Кибератака	Вторая по размерам сеть некоммерческих госпиталей в США испытывала проблемы с работой ИТ-сервисов более недели. Часть данных была утеряна. Цена аварии превысила $150 млн
AWS (США)	4	2022 (III)	Потеря электропитания / авария переключателя	Нарушение работы основной зоны доступности AWS отразилось на тысячах бизнес-пользователей. Каскадирование ошибок при восстановлении затронуло сторонние сервисы
Национальная служба здравоохранения (Великобритания)	4	2022 (III)	Перегрев / авария системы охлаждения	В одном из крупнейших госпиталей NHS в Лондоне была нарушена работа всех сервисов. Цена простоя – £1,4 млн
Microsoft (Европа/ глобально)	4	2022 (III)	Потеря электропитания / авария переключателя	Заказчики, в основном из Западной Европы, столкнулись с большими задержками и нарушением доступа к приложениям Microsoft 365

Источник: Uptime Institute Intelligence, 2023



Источник: Uptime Institute Global Survey of IT and Data Center Managers, 2019–2022

▲ Рис. 6. Цена отказов ЦОДов

Цена отказов

Данные, полученные нами в ходе исследований за несколько лет, ясно показывают, что простои обходятся все дороже. В глобальном опросе 2022 г. четверть респондентов заявили, что прямые и косвенные издержки их последнего отключения превысили $1 млн (рис. 6). Это подтверждает тенденцию к росту стоимости инцидентов. Еще 45% респондентов заявили, что последнее отключение обошлось им в сумму от $100 тыс. до $1 млн. Очевидно, аргументы в пользу увеличения инвестиций в отказоустойчивость (и обучение) становятся все более вескими.

Почему цена отказов увеличивается? Это может быть связано с целым рядом факторов, начиная от инфляции, повышения штрафов за нарушения SLA, стоимости рабочей силы, запасных частей и их замены, но самая главная причина – растущая зависимость экономической деятельности компаний от цифровых сервисов и ЦОДов. Потеря критически важной ИТ-службы часто напрямую и незамедлительно приводит к сбоям в работе бизнеса и потере доходов.

Мы не рассчитываем среднюю стоимость простоев, поскольку полученная информация редко бывает полезной – последствия сбоев сильно различаются для разных отраслей и предприятий. Каждый год несколько крупных аварийных отключений обходятся настолько дорого, что могут исказить общую картину. Некоторые из них влекут за собой компенсации, штрафы и потерю бизнеса, а затраты исчисляются миллионами или даже десятками миллионов долларов. В 2022 г. стало известно о нескольких отключениях, которые обошлись более чем в $150 млн.

Тенденция к росту затрат, связанных с отказами в ЦОДах, вероятно, сохранится, поскольку зависимость от цифровых услуг увеличивается. Более строгие соглашения SLA, на которых настаивают многие заказчики, могут сделать перебои в работе ЦОДов еще более дорогостоящими для их владельцев/операторов, а также привести к повышению штрафов регулирующих органов и компенсаций клиентам. Это также оправдывает увеличение инвестиций в обеспечение отказоустойчивости.

Выводы

Высокая доступность и отказоустойчивость (что означает предотвращение простоев и эффективное восстановление) – приоритетные цели для всех участников рынка цифровой инфраструктуры. Иногда думают, что прогресс в этой области остается столь же непременным, как закон Мура в последние три десятилетия. Но это не так: наши данные показывают, что улучшения достигаются с трудом, а сбои обходятся все дороже. Более того, некоторые тенденции могут свести на нет достижения в повышении надежности оборудования и совершенствовании процессов эксплуатации и управления.

Во-первых, переход к распределенным архитектурам, когда все больше ИТ-функций выполняется в стандартных ИТ-системах, часто распределенных или реплицируемых на многих сайтах, конечно, снижает влияние некоторых локализованных сбоев. Но он также может вызвать дополнительные проблемы с сетью, ПО или самими ИТ-системами.

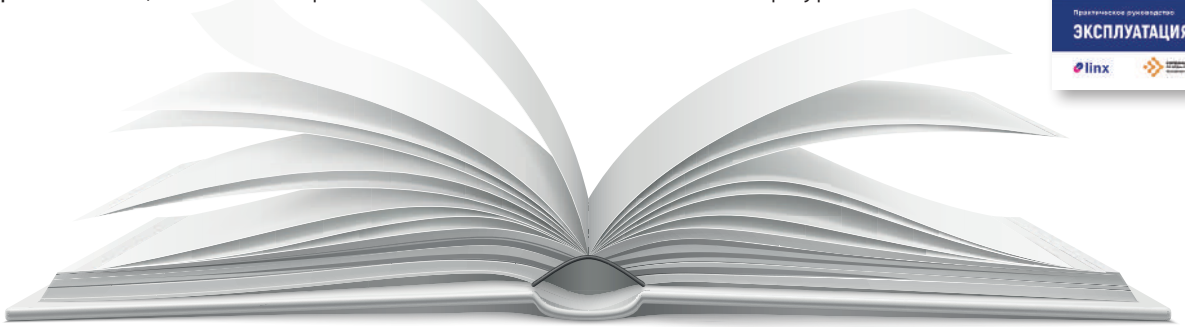
Во-вторых, переход к возобновляемым источникам энергии и распределенной генерации и хранению энергии, по мнению многих экспертов, снизит надежность электросети. Хотя сбои в электросетях не считаются основной причиной отказов в работе ЦОДов, они создают дополнительную нагрузку на их энергосистемы и процессы управления.

В-третьих, роль опытного и хорошо обученного персонала, который следует проверенным процессам управления, имеет решающее значение для обеспечения отказоустойчивости. Однако во многих регионах наблюдается серьезная нехватка квалифицированных кадров.

Предотвращение отказов в ЦОДах – это задача, требующая постоянного мониторинга и внимания, инвестиций и анализа. Ключевые составляющие ее решения: повышение уровня резервирования, тестирование, постоянный анализ меняющихся угроз и новых технологий и, возможно, прежде всего инвестиции в персонал и обучение. ИКС

Служба эксплуатации ЦОД*

Тарас Чирков, директор по эксплуатации ЦОД, Linx Datacenter
Константин Нагорный, главный инженер Linx Datacenter в Санкт-Петербурге
Андрей Чеснов, главный энергетик Linx Datacenter в Санкт-Петербурге



Продолжая знакомить читателей «ИКС» с фундаментальными работами по тематике дата-центров, написанными экспертами отрасли, предлагаем вашему вниманию главу из книги «Эксплуатация ЦОД. Практическое руководство», которая выходит в свет в марте 2024 г. в издательстве «Альпина Паблишер».

Прежде всего мы должны установить и определить, что такое служба эксплуатации ЦОД.

Служба эксплуатации — это ключевое структурное подразделение ЦОД, команда которого, эксплуатируя инженерное оборудование и системы согласно действующим нормам, правилам и стандартам, обеспечивает предоставление услуг заранее определенного уровня.

Многие считают, что служба эксплуатации отвечает в ЦОД за все. Это, конечно же, не так. Служба эксплуатации отвечает за работу критически важных **инженерных** систем, список которых приведен в соответствующей главе. Важно понимать, что служба эксплуатации не отвечает за сети передачи данных (за исключением прокладки и коммутации кабелей) и серверное оборудование с программным обеспечением (за исключением подачи электричества и охлаждения).

Служба эксплуатации ЦОД вообще может не представлять, какие именно данные обрабатываются на серверах, размещенных в ЦОД (особенно актуально для коммерческих ЦОД), но должна понимать совместно с клиентом, что необходимо обеспечить, чтобы эти серверы работали.

Задачи службы эксплуатации ЦОД

В действующем Своде правил (СП) «Здания и сооружения. Правила эксплуатации. Основные положения» можно найти достаточно верное определение службы эксплуатации:

Служба эксплуатации зданий (сооружений) обеспечивает самостоятельно или с привлечением специализированных организаций выполнение комплекса работ по эксплуатационному контролю и обслуживанию зданий (сооружений):

- участие при вводе в эксплуатацию здания (сооружения) с правом визирования документов;
- взаимодействие с организациями, выполняющими монтажные и пусконаладочные работы..;
- поддержание эксплуатационных показателей строительных конструкций зданий (сооружений)..;
- эксплуатационный контроль и обслуживание систем инженерно-технического обеспечения..;
- круглосуточное диспетчерское обслуживание систем инженерно-технического обеспечения и коммуникаций..;
- эксплуатацию производственного оборудования..;
- при необходимости создание собственной службы по обеспечению работ по устранению аварийных ситуаций и своевременный вызов аварийных служб в случае невозможности ликвидировать аварийную ситуацию собственными силами;
- исполнение нормативных актов, нормативных документов и технической документации по эксплуатации собственными силами или с привлечением сторонних организаций;
- ведение технической эксплуатационной документации, в том числе внесение изменений, возникших при эксплуатации объекта..;

*Публикуется с сохранением особенностей орфографии и редактуры издательства.

- взаимодействие с подрядными организациями и контроль их работы;
- работы по уборке и благоустройству территории...[22]

Несмотря на то, что здесь описывается служба эксплуатации зданий, по своей сути ее задачи не отличаются от службы эксплуатации ЦОД. Забегая вперед, можно сказать, что тут указаны почти все аспекты деятельности ЦОД, которые будут раскрыты далее.

В свою очередь, европейский стандарт EN50600–3–1 эту же задачу выражает более емко одной фразой:

> The aim... is to keep the data center at the status of normal operations[23].

Давайте попробуем сформулировать основные задачи, характерные для ЦОД:

- Предоставление потребителям услуг определенного уровня согласно SLA/OLA.
- Организация **постоянно совершенствующихся** процессов эксплуатации согласно действующим нормам, правилам и международным стандартам.
- Раскрытие всего потенциала инженерных систем и рациональное расходование ресурсов.

Наверняка вы можете назвать и другие задачи; ниже мы приводим аргументы, почему мы в качестве задач выбрали именно эти.

Предоставление услуг клиентам согласно SLA

Данная задача является «вершиной пирамиды» работы службы эксплуатации. Клиенты должны получать услуги с параметрами, прописанными в договоре.

Для расстановки приоритетов внутри службы эксплуатации на случай устранения нескольких одновременных инцидентов можно разделять критичность различных параметров SLA. Например, краткосрочное отключение электропитания стойки, очевидно, намного критичнее долгосрочного незначительного превышения уровня влажности, хотя с формальной точки зрения ЦОД должен предоставить именно те уровни сервиса, которые прописаны в договоре, независимо от их критичности для оборудования клиента. Именно за нарушение SLA с клиентами руководители и сотрудники службы эксплуатации ЦОД должны лишаться премий или увольняться в первую очередь, и, напротив, их нужно поощрять за отсутствие таких нарушений. Подробнее об этом написано в главах «Мотивация и KPI» и «Потребители услуг ЦОД и важность SLA».

[22] СП 255.1325800.2016 Здания и сооружения. Правила эксплуатации. Основные положения (с Изменениями № 1, 2).
[23] EN50600–3–1:2016 Information technology — Data centre facilities and infrastructures, p. 7.2.1

Организация процессов эксплуатации

По действующим нормам и правилам

Это классическая задача для службы эксплуатации любого предприятия. Мы работаем в правовом поле, требующем от нас соблюдения правил электробезопасности, пожарной безопасности, охраны труда и т. п. Сотрудники должны быть обучены и аттестованы исходя из требований к эксплуатируемому оборудованию, документация должна вестись надлежащим образом. Если этого не происходит, есть риск получения законных претензий со стороны контролирующих органов, от штрафов до приостановки деятельности. Служба эксплуатации всегда должна быть готова пройти любой аудит со стороны надзорных органов.

Так как задача организации процессов службы эксплуатации согласно нормам и правилам – типовая для любого предприятия, то она должна быть на 100% качественно выполнена службой эксплуатации, а требования норм и правил рассматриваются как необходимый минимум для безопасного и качественного построения всех остальных процессов эксплуатации.

По требованиям международных стандартов и best practice[24]

Опыт показывает, что соблюдение норм и правил – только фундамент для организации процессов. Дальше необходимо выбрать ту модель построения процессов службы эксплуатации, которая обеспечит требуемую надежность. Данная модель определяет экосистему документации и процессов, их взаимосвязь между собой. При этом важно избежать двойной документации, совместив документацию «для норм» с документацией для best practice. Служба эксплуатации всегда должна быть готова пройти любой аудит со стороны независимых аудиторов.

На данный момент общепринятой эффективной best practice моделью является Method of Procedure (MOP). Если изучить его историю, то становится понятно, что данный метод не придуман специально для ЦОД, а пришел из других, более старых объектов критической инфраструктуры, в частности, с морского флота. Далее мы очень подробно рассмотрим все аспекты этого метода.

Раскрытие всего потенциала инженерных систем и рациональное расходование ресурсов

Пункт 1.2.2 ПТЭЭП[25] обязывает: «*Потребитель обязан обеспечить учет, рациональное расходование электрической энергии и проведение мероприятий по*

[24] Лучшая практика» (англ.). Устоявшееся универсальное название для комплекса знаний, мер и навыков, применяемых в той или иной сфере для достижения максимальной эффективности какого-либо процесса или действия.
[25] Правила технической эксплуатации электроустановок потребителей (ПТЭЭП), в редакции до 2022 г.

энергосбережению». Пункт 1.5.1 ПТЭЭП гласит: *«Система управления электрохозяйством Потребителя электрической энергии... должна обеспечивать: ...эффективную работу электрохозяйства путем совершенствования энергетического производства и осуществления мероприятий по энергосбережению»*.

В распоряжении службы эксплуатации ЦОД находятся высокотехнологичные инженерные системы с заложенной в них избыточностью (резервированием). Грамотно выстроив процессы эксплуатации, необходимо использовать этот, заложенный в системы, потенциал, для недопущения влияния аварий единичного оборудования на итоговый уровень SLA перед клиентами.

Любое оборудование имеет оптимальные параметры работы, при которых соблюдается баланс между эффективностью и износом. Если откинуть пафос слов о природе и глобальном потеплении, нужно просто помнить, что в руках службы эксплуатации ЦОД находится условный нагревательный прибор, мощность которого измеряется в мегаваттах. Незначительными настройками оборудования и режимов его работы, даже без влияния на надежность, можно легко варьировать мощность этого нагревательного прибора в разумных пределах. А если помнить, что таких нагревательных приборов в мире все больше и больше, то становится очевидным, что режимы работы оборудования должны быть выбраны таким образом, чтобы обеспечивать требуемую надежность, но при этом не расходовать лишнюю энергию.

Роль службы эксплуатации на различных этапах построения ЦОД

Перед началом непосредственного использования объект нужно построить, протестировать и сдать в эксплуатацию. Чтобы переход от построения ЦОД к эксплуатации был максимально гладким и организованным, а уровень сервиса — высоким с первых дней работы ЦОД, требуется участие службы эксплуатации на всех этапах создания ЦОД, начиная с написания технического задания. Надо учитывать, что служба эксплуатации не обладает таким опытом, как проектные организации, сдающие по несколько ЦОД в год, но тем не менее она определяет важные нюансы, которые улучшат или облегчат функционирование ЦОД в дальнейшем.

Поэтому крайне важно начинать формировать службу эксплуатации еще до начала работ по проектированию ЦОД, чтобы иметь свою внутреннюю команду для контроля выполнения задач проектировщиками. Эта команда будет максимально заинтересована в получении результата – ведь именно ей в дальнейшем придется эксплуатировать данный ЦОД.

Какие задачи будут выполняться на начальном этапе:

Планирование, дизайн

- Разработка концепции ЦОД, исходя из потребностей клиента (требуемый уровень доступности, резервирования и т.д.)
- Принятие решения о необходимости организации службы эксплуатации ЦОД, объемах выполнения задач
- Участие эксплуатации в проектировании
- Разработка проектной документации (согласованы уставки, наименования, принципы маркировки оборудования)
- Создание SCP* (конфигураций режимов работы оборудования)

Строительство ЦОД

- Маркировка оборудования, положений выключателей/задвижек «по умолчанию»
- Разработка необходимой для получившейся инфраструктуры концепции SOP, MOP, EOP на основании SCP, проектных документов, раскладки здания/помещения ЦОД и сопутствующей инфраструктуры, информации от вендоров по техническому обслуживанию оборудования

Приемка, тестирование

- Разработаны необходимые для старта документы эксплуатации. Определены возможные аварийные ситуации для наполнения EOP
- Проведены тренировки по штатному и внештатному режиму работы оборудования (удачный этап, так как есть возможность получить нагрузку без клиентского оборудования и потренировать команду)
- Многосоставные приемные испытания

Эксплуатация

- Функционирование ЦОД в режиме эксплуатации, с поддержанием и обновлением всего пакета документации
- Разработка методов взаимодействия с клиентами
- Проактивная работа с инцидентами, расширение списка EOP
- Оптимизация и совершенствование процессов

* Значение аббревиатур SCP, SOP, MOP, EOP будет объяснено далее по тексту.

Пусконаладочные работы, приемка в эксплуатацию

После того как ЦОД построен, он проходит пусконаладочные работы и приемо-сдаточные испытания, которые являются начальной точкой эксплуатации и предваряют дальнейшее повседневное управление ЦОД. Собственно пусконаладочные работы, испытания и сдача ЦОД в эксплуатацию (commissioning) состоят из нескольких достаточно широко известных этапов, которые, в частности, предлагает Uptime Institute:

1. **Заводское тестирование производителем** критически важного инженерного оборудования (Factory Acceptance Test, FAT, или Factory Witness Test, FWT). Может быть проведено как в присутствии представителя команды эксплуатации, так и без него, с приложением результатов заводского тестирования к комплекту документов.
2. **Получение, установка и предварительное функциональное тестирование** критически важного инженерного оборудования (Installation Acceptance Test, IAT). Получение, первичная установка оборудования, оценка комплектности и соответствия спецификации, проверка правильности монтажных работ в соответствии с проектом.
3. **Функциональное тестирование, автономное тестирование** критически важного инженерного оборудования и начальная конфигурация предварительного пуска системы (Component Test, CT). Настройка и тестирование оборудования.
4. **Запуск системы, OEM-тестирование и индивидуальное тестирование систем** (Site Acceptance Test, SAT). Испытания конкретного оборудования по соответствующей программе, с нагрузкой и без.
5. **Интегрированные эксплуатационные испытания** (Integrated Site Acceptance Test, ISAT). Комплексные испытания всех систем ЦОД одновременно на расчетную нагрузку.

Важно понимать, что все эти стадии приемки оборудования в эксплуатацию происходят не только во время начала работы ЦОД, но и при всех последующих расширениях различных систем.

Влияние службы эксплуатации на проектирование

В процессе создания ЦОД каждый должен выполнять свою роль. Часто между проектировщиками и службой эксплуатации возникают споры из-за технических решений. И на самом деле споры – это хорошо. Если люди готовы слушать аргументы, то в спорах рождается лучшее решение.

Ниже опишем некоторые часто встречающиеся примеры из нашей практики, неочевидные для проектировщиков и жизненно важные для эксплуатации и потребителей услуг ЦОД.

Требования к внешнему электроснабжению

Зачастую заказчики и проектировщики пытаются повысить надежность проектируемого ЦОД путем ужесточения требований к внешнему электроснабжению. В результате напрасно расходуется время на поиски площадки с возможностью выделения двух независимых городских вводов электричества для обеспечения первой или второй категории надежности энергоснабжения[26], при этом подключение по более высокой категории оплачивается по повышенным ставкам (технологическое присоединение по второй категории надежности будет значительно дороже по сравнению с третьей). Кроме того, срок технологического присоединения увеличится, так как для присоединения по более высокой категории потребуется больше времени на проектирование, согласование проекта в Ростехнадзоре и получение разрешительных документов. При этом подходящие площадки, имеющие только один ввод внешнего электроснабжения, отвергаются априори.

Однако если открыть стандарт Tier Standard: Topology (TS: T) компании Uptime Institute, то мы увидим в пункте 2.5, что «*энергогенерирующие системы площадки (например, двигатель-генераторы, топливные элементы) рассматриваются в качестве основного источника электроснабжения ЦОД. Местная электрическая сеть является экономичной альтернативой...*».

Далее, если мы обратимся к статье «Система классификации Tier: мифы и заблуждения»[27], то узнаем, что, «*согласно стандарту Tier Standard: Topology, единственным надежным источником электропитания для ЦОД является генераторная установка. Это связано с тем, что электроснабжение подвержено незапланированному отключению даже в местах с надежными электросетями. Число внешних фидеров, подстанций и электросетей, к которым подключен ЦОД, не определяет его уровень Tier и никак не влияет на него. Как следствие, подключение к электросети общего назначения даже не требуется для сертификации*».

К этому выводу можно было прийти и самостоятельно, просто внимательно прочитав определение категорий электроснабжения в Правилах устройства электроустановок (ПУЭ).

*ПУЭ, п. 1.2.19. Электроприемники первой категории в нормальных режимах должны обеспечиваться электроэнергией от **двух независимых взаимно резервирующих источников питания**, и перерыв их*

[26] О категориях надежности энергоснабжения электропотребителей см. Правила устройства электроустановок (ПУЭ), один из основополагающих документов при построении систем энергоснабжения инженерных объектов.

[27] Хэслин К. Система классификации Tier: мифы и заблуждения. 29.05.2019. Перевод: https://dcforum.ru/news/sistema-klassifikatsii-tier-mify-i-zabluzhdeniya, оригинал (англ.): https://journal.uptimeinstitute.com/myths-and-misconceptions-regarding-the-uptime-institutes-tier-certification-system/.

электроснабжения при нарушении электроснабжения от одного из источников питания может быть допущен лишь ***на время автоматического восстановления питания****.*

ПУЭ, п. 1.2.20. Электроприемники второй категории в нормальных режимах должны обеспечиваться электроэнергией от ***двух независимых взаимно резервирующих источников питания****. Для электроприемников второй категории при нарушении электроснабжения от одного из источников питания допустимы перерывы электроснабжения* ***на время, необходимое для включения резервного питания действиями дежурного персонала или выездной оперативной бригады.***

В приведенных пунктах ПУЭ мы видим две важные вещи:

А) В обоих случаях источники должны быть взаимно резервирующими, а это те источники, на которых, согласно ПУЭ, п. 1.2.10, «сохраняется напряжение в послеаварийном режиме в регламентированных пределах при исчезновении его на другом или других источниках питания», то есть резерв источников должен быть 2N. Не следует путать это резервирование с двумя линиями от одной подстанции (резерв линий 2N). Наличие резерва 2N по линиям от одного источника, например от ДГУ, вполне логично, так как позволяет обслуживать одну линию без выведения всего комплекса ДГУ из работы. Наличие двух линий от городской подстанции тоже имеет смысл, так как позволит вам не переходить на ДГУ при обслуживании одной из этих линий. Но две линии от одного источника – это все равно третья категория надежности.

Б) Время пропадания электричества равно времени ручного переключения для второй категории и времени автоматического переключения – для первой. При этом в обоих случаях пропадание **допустимо** и **время этого переключения не нормировано**, хотя, скорее всего, предполагается, что время ручного переключения исчисляется в минутах (а может, и в часах), а автоматического – в секундах, если другое явно не указано в договоре на электроснабжение. Теперь представьте себе, что электроснабжающая организация согласится добавить себе в договор дополнительные временные обременения и, естественно, штрафы за их неисполнение, а они равны штрафам, которые клиенты выставят ЦОД. Считаете ли вы такое развитие событий вероятным?

Подведем итог:

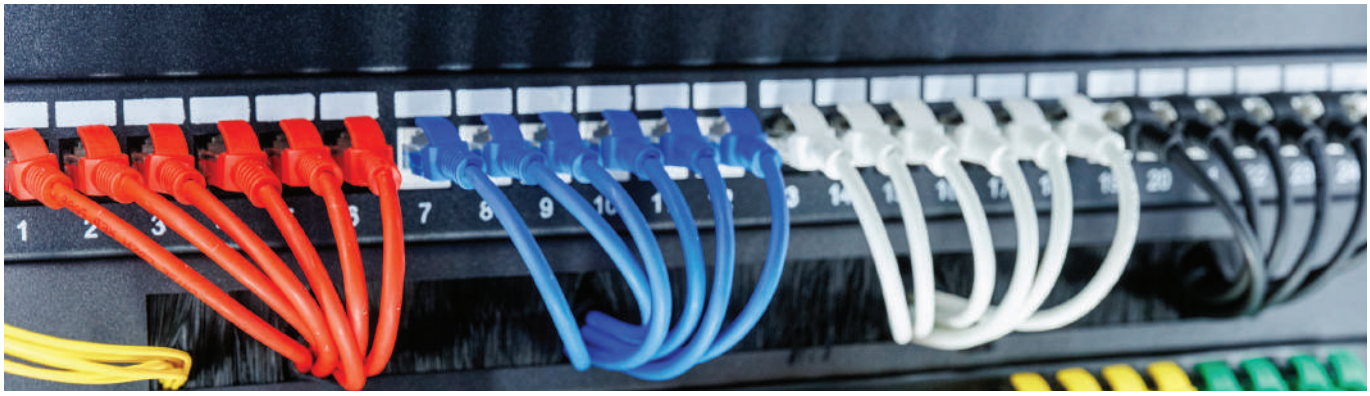
1. При любой категории внешнего электроснабжения надо понимать, что его безотказная работа находится не в вашей зоне ответственности. Другое дело – всецело принадлежащий вам источник электроснабжения (чаще всего это ДГУ). За его состояние и работоспособность несет ответственность служба эксплуатации, то есть вы сами.

2. Согласно Uptime Institute Tier Standard: Topology (TS: T), п. 2.5, «*перебои в электрической сети (внешней) считаются не аварийной ситуацией, а ожидаемым рабочим условием, к которому площадка полностью подготовлена*». Подготовить площадку к такому событию возможно путем проведения плановых работ по переключению на локальные источники генерации электричества и обратно с целью убедиться в надежной работе такого переключения. Однако, по нашему опыту, во многих ЦОД опасаются производить настоящее отключение внешнего электроснабжения для тестирования ДГУ, а следовательно, и тестирования всей энергосистемы в комплексе, считая, что такое переключение может пройти со сбоями и повлиять на сервисы, предоставляемые клиентам. Тем не менее без регулярного проведения таких полноценных запусков ДГУ быть уверенным в безотказной работе ЦОД не представляется возможным.

В результате мы видим, что, с точки зрения стандарта Tier Standard: Topology, категория электроснабжения ЦОД никак не влияет на уровень надежности ЦОД, а служба эксплуатации ЦОД может рассчитывать только на источники электричества, находящиеся в собственном управлении ЦОД (чаще всего это ДГУ), и должна быть всегда готова к вероятному отключению внешних источников электроснабжения, которые рассматриваются как вспомогательные. Однако это утверждение не отменяет положительного влияния на надежность, которое дает наличие двух взаиморезервирующих вводов электроснабжения площадки от одного источника энергии или подстанции. Эту схему нельзя называть второй категорией электроснабжения, так как источник один, но она позволяет сохранять электроснабжение площадки при аварии или обслуживании снабжающих площадку линий, ячеек, трансформаторов. При наличии одной кабельной линии вся нагрузка будет запитана только через нее. Получается единая точка отказа: это либо трансформатор, либо кабельная линия, либо вводной автомат. При отказе одного из этих элементов потребуется долгосрочный и дорогостоящий ремонт, а вы все это время будете вынуждены работать от собственных источников – ДГУ. В итоге использование двух независимых кабельных линий – это хорошо, но дорого. Однако стоит понимать, что при выборе второй или первой категории надежности стоимость подключения возрастает минимум в два раза относительно присоединения по третьей категории надежности. Ведь для энергоснабжения по первой или второй категории необходимы два источника питания, а присоединение к каждому из них стоит примерно одинаково.

Окончание главы из книги Т. Чиркова, К. Нагорного и А. Чеснова читайте в следующем номере «ИКС»

Импортозамещение сетевого оборудования: успехи и пробелы



Николай Носов

Отечественные вендоры в целом смогли заместить сетевые решения покинувших российский рынок зарубежных компаний, хотя производимые ими продукты зачастую отличают меньшая надежность, сложность в настройке, неудобство использования и ограниченный функционал.

Уход зарубежных вендоров

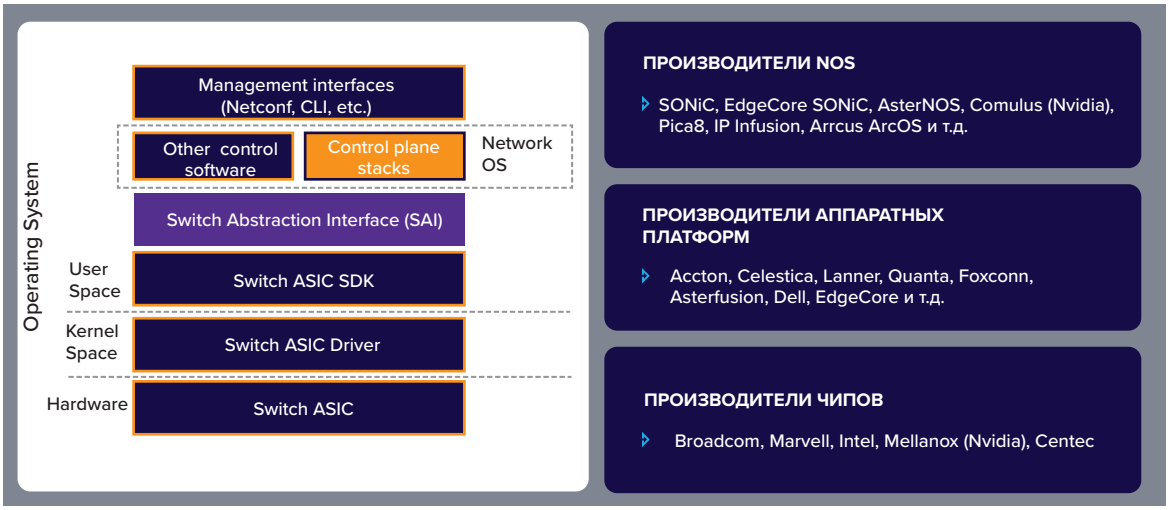
Несмотря на принятую еще в 2014 г. программу импортозамещения, на российском рынке сетевого оборудования долгое время доминировали зарубежные решения. Процесс импортозамещения шел медленно и часто сводился к замене решений вендоров из недружественных стран – Cisco, Juniper – на продукцию дружественной китайской Huawei, которая предлагала всю линейку сетевых устройств.

Уход ведущих мировых вендоров после февральских событий 2022 г. стал для российских компаний серьезным вызовом (рис. 1). Надежды на китайского гиганта не оправдались: Huawei, сама находящаяся под американскими санкциями, заморозила работу на российском рынке. «Образовался некий вакуум, причем не только в оборудовании, но и в вендорском обучении, быстром R&D-процессе, технической поддержке. И самое главное – пропала коммуникационная составляющая», – констатировал на конференции IT Elements 2023 директор Центра сетевых решений компании «Инфосистемы Джет» Сергей Андронов.

Сетевое оборудование мировых гигантов по-прежнему широко используется российскими компаниями, но уже появилось понимание, что вечно так продолжаться не может. Оборудование ломается, требует ремонта, стареет. Выявленные уязвимости надо устранять, обновлять ПО, что особенно важно в условиях резко возросшего числа хакерских атак. Трудно рабо-

Рис. 1. **Поставщики оборудования для сетей передачи данных** ▼

Источник: «Инфосистемы Джет»



◀ Рис. 2. Вендоры, присоединившиеся к проекту OCP

Источник: «Инфосистемы Джет»

тать без привычных сопровождения и поддержки, которые сложно получить в случае параллельного импорта. Да и небезопасно эксплуатировать официально не поставляемые в страну устройства: нет гарантии, что их не отключат удаленно. Поэтому даже не испытывающие давления регуляторов компании озаботились импортозамещением.

«Белый ящик» и проблемы «железа»

Сетевое устройство – совокупность программных и аппаратных средств, главным из которых является процессор. С микроэлектроникой в стране ситуация сложная, серьезно вливать деньги в отрасль стали только с лета 2022 г. Единственный полностью отечественный процессор – «Эльбрус», корни разработки которого уходят еще в советское прошлое. Российским процессором общего назначения можно считать «Байкал», но лицензия на используемую в нем ARM-архитектуру принадлежит зарубежным компаниям. Общее слабое место этих процессоров – зарубежное производство. По нему и ударили: тайваньская компания TSMC присоединилась к санкциям и выпуск российских процессоров прекратила.

Гром грянул, мужик перекрестился. В 2022 г. в Зеленограде приступили к строительству фабрики, которая, по плану, будет выпускать процессоры по 28-нм техпроцессу. Так что есть надежда, что к 2030 г. технология, по которой Huawei уже сейчас производит чипы для своих сетевых устройств, будет освоена. Однако локальное производство процессоров «Эльбрус» не решит всех проблем с сетевым оборудованием – для российской платформы потребуется еще написать операционную систему.

Лучше ситуация с коммутаторами на основе открытой архитектуры. Сегодня многие производители присоединились к проекту Open Compute Project (OCP) и, поддерживая подход white box («белый ящик»), стали выпускать сетевые устройства с разделением программного и аппаратного обеспечения (рис. 2). На них можно устанавливать «отвязывающую» софт от конкретной аппаратной реализации вендора сетевую операционную систему с открытым исходным кодом (самая распространенная в настоящее время – SONiC).

Коммутаторы white box поддерживают программируемость аппаратной плоскости данных (data plane) и контейнерное развертывание ПО. Программно определяемая логика пересылки данных позволяет быстро проводить обновления, повышать гибкость и производительность сети, что особенно удобно в случае облачных вычислений. Унификация с помощью контейнерного развертывания функций управления и эксплуатации снижает затраты на обслуживание сети. Для таких решений можно использовать ресурсы открытого сообщества ONF (Open Networking Foundation), продвигающего разработку и внедрение связанных с программно определяемыми сетями (Software Defined Network, SDN) технологий в коммутаторах white box.

При этом подходе российские компании получают возможность легально покупать качественное «железо», такое же, как у лидеров мирового рынка, и устанавливать на него открытое ПО, по сути то же, что у компаний с известными брендами. На аппаратном уровне остается закрытый код, но в целом контроль за устройством повышается, что важно для служб информационной безопасности.

Российские вендоры аппаратных сетевых решений

Минусы white box в том, что продукты с открытым исходным кодом надо «уметь готовить»: иметь экспертизу и квалифицированных специалистов, способных «допиливать» софт под конкретный проект. Бизнесу проще взять

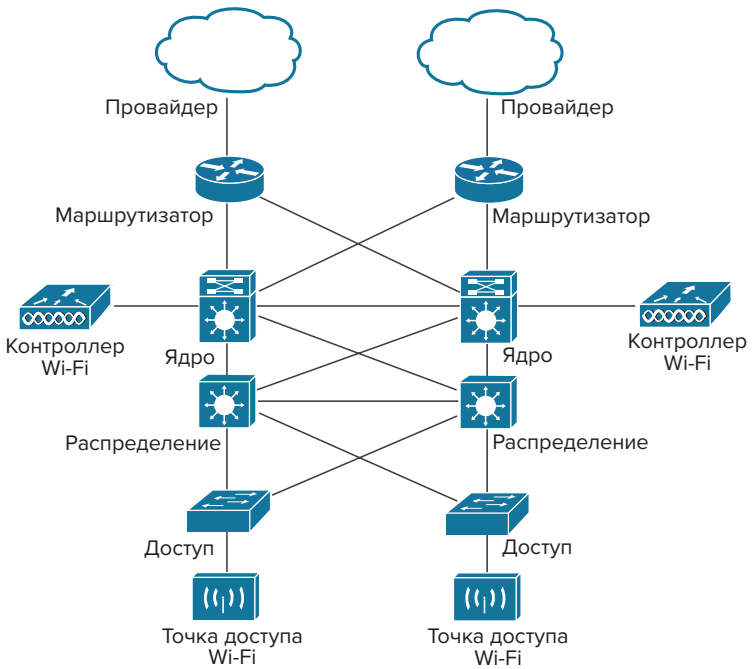
готовый продукт с поддержкой вендора, и такие вендоры на российском рынке есть.

На решениях российских вендоров уже можно построить типовую корпоративную сеть (рис. 3). Для этого есть все необходимое: обеспечивающие соединение с провайдером маршрутизаторы; предназначенные для подключения конечных пользователей коммутаторы доступа; управляющие потоками данных в центре сети коммутаторы ядра; осуществляющие балансировку и оптимизацию трафика сети коммутаторы распределения; контроллеры и точки доступа Wi-Fi.

Так, «Ростелеком», по словам Владимира Каплина, начальника отдела системной архитектуры этой компании, еще до февральских событий начал использовать сетевое оборудование российского производителя «Элтекс». Из-за часто меняющейся у вендора элементной базы приходится тщательно тестировать каждую модификацию сетевого устройства, но работать можно. Главный плюс российских вендоров – хорошая техподдержка, оперативная доработка прошивки и быстрая реакция на выявленные проблемы.

У «Элтекса» есть производственные линии в Новосибирске, на которых сетевые устройства собирают из закупаемых за рубежом микросхем, а не меняют наклейки на коробках китайских производителей. В предлагаемую компанией номенклатуру входят маршрутизаторы, беспроводные точки доступа, шлюзы, IP-АТС, оптические трансиверы, коммутаторы, в том числе коммутаторы для ЦОДов, на которых можно строить сетевые фабрики. В ведущийся Минпромторгом реестр телекоммуникационного оборудования, произведенного на территории РФ, также входят коммутаторы компаний «Информтехника и Связь», НПП «Полигон» и Qtech. Кроме того, в числе российских производителей сетевого оборудования – компании «Вектор-Т», «Натекс», Fplus, N3COM, Utinet.

Рис. 3. Архитектура типовой корпоративной сети ▼



Линейки российских производителей сетевого оборудования расширяются, но отставание от мировых лидеров сохраняется. Нередко отечественные устройства менее надежны и менее удобны в использовании, сложнее в настройке и имеют ограниченный функционал. Есть и проблемы сопровождения – не всегда его можно осуществить удаленно, и тогда требуется выезд специалиста на зачастую далеко расположенный объект.

Сетевая безопасность

Передача данных по внешним каналам сопряжена с рисками утечки информации и атак на внутреннюю инфраструктуру организации через точку подключения к внешней сети. Для защиты от вторжений используются межсетевые экраны. Наиболее надежную защиту обеспечивают межсетевые экраны следующего поколения (Next Generation Firewall, NGFW), сочетающие в себе функциональность межсетевого экрана, антивируса, системы защиты от вторжений, спам- и контент-фильтров. На смену продукции мировых лидеров – Fortinet, Palo Alto Networks, Check Point Software Technologies, Cisco – идут отечественные решения. Среди российских лидеров: компании «Код безопасности», UserGate, «ИнфоТеКС» и «Айдеко». В последнее время в борьбу за рынок NGFW активно включились Positive Technologies и «Солар».

Лучшая защита от утечек – шифрование передаваемых данных, в частности, с использованием криптошлюзов. Импульс внедрению российских криптошлюзов в бизнес дало принятие еще в 2006 г. закона «О персональных данных», после чего на российскую криптографию стали массово переходить банки. В настоящее время для защиты передаваемых по внешним каналам данных широко применяются аппаратно-программные криптошлюзы российских вендоров, например, «ИнфоТеКС» и «С-Терра СиЭсПи».

SDN и виртуализация сетевых фабрик

Виртуализация вычислительных средств повышает эффективность их использования, гибкость и масштабируемость. Это справедливо и для программно определяемых сетей, в которых слой «железа» отделяется от слоя управления (control plane).

Но в импортозамещении решений для программно определяемых сетей успехи пока невелики, особенно в случае аппаратной виртуали-

зации, т.е. виртуализации специализированных физических сетевых устройств. При аппаратной виртуализации централизованное управление и программную настройку сетевых коммутаторов и маршрутизаторов осуществляют программно-аппаратные SDN-контроллеры, взаимодействующие с сетевыми устройствами через открытые интерфейсы и протоколы. Программная виртуализация сетей работает на обычных серверах и, как правило, является частью платформы их виртуализации.

Программная виртуализация обычно интегрирована с системой виртуализации и имеет собственные средства для создания наложенной сетевой связности, поясняет Александр Гуляев, главный архитектор по сетевым технологиям компании «Инфосистемы Джет». Для построения топологии и обработки трафика используется функционал туннелей и виртуальных функций. Сети достаточно поддерживать функционал IP-фабрики, предоставляющей базовую L3-связность, которая позволит компонентам решения на различных серверах взаимодействовать между собой.

Аппаратная виртуализация сети ЦОДа означает создание сетевой фабрики на базе коммутаторов, поддерживающих технологию EVPN/VXLAN. На российском рынке есть продукты, в которых заявлен данный функционал, но примеров построения продуктивных EVPN-фабрик на этих продуктах мало. Чаще всего опыт ограничивается тестированием оборудования. В каждом конкретном случае стоит продумать дизайн и проверить соответствие между предполагаемым дизайном и поддерживаемым функционалом.

«Также можно рассмотреть коммутаторы white box, предоставляющие возможность выбора ПО, – добавляет А. Гуляев. – Но в этом случае придется решать проблемы взаимодействия “железа” и ПО разных производителей. В целом в сфере аппаратной виртуализации сети не стоит ожидать быстрых готовых ответов и проверенных решений. Процесс еще в стадии становления».

Его дополняет Илья Фурцев, начальник отдела поддержки продаж сетевых решений той же компании. «Российских вендоров SDN-решений для ЦОДов и кампусных сетей (не считая SD-WAN) сегодня нет. Основная задача российских производителей – охватить всю линейку зарубежных вендоров. Для создания полноценного отечественного SDN-решения может потребоваться около пяти лет», – считает он. «Нет и пока не планируется», – подтвердили вывод эксперта ряд представителей российских поставщиков аппаратных сетевых решений.

В Едином реестре российских программ для ЭВМ и баз данных (ЕРРП) в 2022 г. зарегистрирован контроллер RunOS – продукт для программно конфигурируемых сетей от «РанСДН» (RunSDN), стартапа Центра прикладных исследований компьютерных сетей, резидента «Сколково». Контроллер RunOS был создан еще в 2014 г., а в 2016 г. было анонсировано его пилотное внедрение на сети «Ростелекома» в одном из регионов России. На сайте компании решение аттестуется как самое быстрое из всех существующих в мире программно конфигурируемых контроллеров и заявляется, что подтверждена его совместимость с устройствами производителей Arista, Juniper, Extreme Networks, NEC, IBM и Huawei. Однако подтверждающих документов на сайте нет, на запросы редакции компания не ответила.

Наложенные сети

С импортозамещением программной виртуализации сети дело обстоит лучше. Можно использовать продукты open source, например, плагины сетевой виртуализации OpenStack – OVN (Open Virtual Network), что и делают сейчас многие российские облачные провайдеры, решившие отказаться от зарубежных проприетарных продуктов. Заменить весь функционал VMware NSX можно с помощью дополнительных open source-компонентов, например, виртуальных межсетевых экранов, роутеров. Но это все не коробочные, а проектные решения. Для каждой задачи нужно выбрать релиз и версию OpenStack.

Чтобы использовать open source-решения в рабочей версии продукта, нужно иметь в штате квалифицированных программистов. Это могут позволить себе в основном крупные компании – бизнес непрофильный, да и специалистов найти непросто. Проще прибегнуть к помощи интеграторов, разворачивающих решения, например облачные, на платформах российских вендоров. Конечно, интеграторы будут опираться на open source-продукты, но обеспечат их работоспособность и смогут внести необходимые корректировки.

Российские решения программной виртуализации сети предлагаются не как отдельный продукт, а как часть платформы виртуализации. Так, по утверждению ITglobal.com, разработчика гиперконвергентной платформы vStack, весь код используемой SDN (разворачивается на каждом узле – физическом сервере гиперконвергентной системы) написан программистами компании.

Работу программной виртуализации можно показать на примере российской программно определяемой сети компании «Орион» (Orion soft), входящей в платформу серверной виртуализации zVirt. В компании рассказали, что хосты виртуализации при установке формируют меж-

Линейки российских производителей сетевого оборудования расширяются, но отставание от мировых лидеров сохраняется

ду собой туннели типа «точка – точка». Таким образом организуется оверлейная сеть, работающая поверх физической. Весь SDN-трафик при необходимости покинуть область работы гипервизора будет передаваться по ней. Далее формируются логические сети – аналог VLAN. Для соединения логических сетей между собой используется виртуальный маршрутизатор.

Для подключения виртуальной сети к физической используются два механизма. В первом случае, на уровне L3, логический маршрутизатор подключается к заданному uplink-порту физического коммутатора и выглядит как обычный порт со своим IP-адресом. Во втором, при подключении на уровне L2, виртуальная машина из сети SDN подключается к существующей VLAN и работает так, как будто в ней находится.

Поскольку сеть программно управляемая, в ней легко реализовать микросегментацию. На порт виртуальной машины можно установить межсетевой экран, причем заданные правила будут выполняться вне зависимости от конфигурации виртуальной машины.

Виртуализация глобальных сетей

В случае глобальных сетей используется технология SD-WAN. С ее помощью организации могут использовать комбинацию частных и общедоступных сетевых подключений, в проводных и беспроводных сетях для установления безопасных и надежных соединений между своими филиалами, ЦОДами и облачными службами. Отделяя сетевое оборудование от уровня управления, SD-WAN в реальном времени анализирует перегрузку каналов, задержки, качество соединения и маршрутизирует сетевой трафик, обеспечивая оптимальную производительность и надежность.

Сеть – кровеносная система бизнеса, без которой трудно представить даже небольшие предприятия

Одним из пионером на российском рынке SD-WAN стала МТС, начавшая в 2020 г. использовать решения Fortinet. В 2021 г. появилось первое российское решение SD-WAN, выпущенное компанией BI.ZONE. Купив разработчика систем управления сетями передачи данных Brain4Net, в 2022 г. вывела на рынок свое SD-WAN решение «Лаборатория Касперского». В ЕРРП также зарегистрирована основанная на технологии программно определяемых сетей система «Богатка» московского производителя сетевого оборудования Network Systems Group.

В 2023 г. список входящих в ЕРРП решений SD-WAN пополнился продуктом Reasonance от разработчика систем автоматизации НПП «Бизнес Связь Холдинг» (бренд Manticore). Его основное отличие от решений конкурентов в том, что на площадке заказчика необязательно устанавливать дополнительное оборудование. Продукт может интегрироваться в существующую сетевую архитектуру и управлять уже действующим оборудованием клиента. «Опыт работы с заказчиками показал, что не все готовы менять имеющуюся сеть. Мы осуществляем поддержку гибридных мультивендорных сетей, в которых новые локации можно подключать по новой схеме на новом оборудовании с более широкими функциями автоматизации, и при этом не спешить с заменой оборудования на существующих локациях, где будут реализованы ключевые функции для управления», – пояснила заместитель генерального директора НПП «Бизнес Связь Холдинг» Ксения Тольман. Правда, Reasonance не коробочное решение, для интеграции его в уже существующую сеть понадобится дополнительное время на доработку конфигурационных файлов сетевых устройств конкретного вендора.

«Бизнес Связь Холдинг» создала веб-платформу, работающую с сетевым оборудованием компаний Cisco, MikroTik, Fortinet. В ближайшее время появится возможность управлять устройствами китайской Huawei и российской Qtech. Управление осуществляется по защищенным каналам из облака Manticore, либо оркестратор разворачивается на ресурсах заказчика. В результате заказчик может сам управлять сетью SD-WAN, например, переключать критичные для бизнеса сервисы на наиболее надежный канал, диагностировать состояние и управлять функциями одновременно большого количества сетевых объектов. Компания планирует в следующем году предложить и аппаратное решение для заказчиков, готовых к замене парка оборудования.

Не хочется, но придется

Сеть – кровеносная система бизнеса, без которой трудно представить даже небольшие предприятия. «Работает – не трогай» – этой жизненной мудрости придерживаются опытные сисадмины. Не хочется без крайней необходимости отказываться от сетевого оборудования зарубежных вендоров, которое по-прежнему широко используется российским бизнесом. Жаль инвестиции в «железо» и экспертизу, накопленный опыт эксплуатации. Однако риски применения этого оборудования возросли, стало понятно, что поддержки не будет и параллельный импорт не спасет.

Замена на российские решения идет медленно и не всегда возможна без потерь. Трудно требовать от российских вендоров такого же качества и надежности продукции, как у имеющих значительно больший опыт, экспертизу и финансовые возможности мировых лидеров, но вариантов мало. Процессы импортозамещения резко ускорились, дело за российскими производителями. ИКС

Исчерпала ли себя многомодовая оптика в ЦОДе?

Колоссальные объемы данных, «перемалываемые» в ЦОДах, требуют высоких скоростей их передачи и заставляют для организации информационного обмена в машинных залах выбирать волоконно-оптические линии связи. Какой оптике отдать предпочтение: одномодовой или многомодовой?

Андрей Семенов, профессор, МТУСИ

Выбор типа волокна

Сегодня типовая скорость передачи данных в дата-центрах составляет 400 Гбит/с, а оценка перспектив указывает на значение 800 Гбит/с уже к концу текущего десятилетия. При этом действующая нормативная база СКС допускает применение в машинном зале ЦОДа и одномодовой, и многомодовой оптики. С функциональной точки зрения эти варианты равноценны, так как обеспечивают одинаковые скорости передачи данных. Использование того или иного решения целиком и полностью оставляется на усмотрение авторов проекта. Однако при выборе из двух близких вариантов построения линии желательно иметь возможность опереться на какие-либо правила и рекомендации, следование которым позволит минимизировать риски проектной ошибки.

Поэтому ряд специалистов в стремлении радикально решить проблему выбора настаивают на применении во всем ЦОДе только одного типа элементной базы, а именно одномодовой оптики, и используют при этом следующие аргументы:

- фактическое отсутствие ограничений по дальности передачи (минимальная дальность действия одномодовых волоконно-оптических сетевых интерфейсов составляет 500 м, что в несколько раз превышает предельное значение этого параметра для многомодовых вариантов, обеспечивающих не более 150–200 м);
- возможность унифицировать тип применяемой элементной базы внутриобъектовой информационной проводки машзала ЦОДа с соединительными линиями операторов связи.

Эти аргументы, на первый взгляд вполне резонные, при более внимательном рассмотрении оказываются весьма дискуссионными и, на наш взгляд, не могут считаться достаточными для столь радикальной коррекции принципов построения физического уровня информационной системы машинного зала ЦОДа.

Во-первых, для рассматриваемой области применения предельная дальность связи в сотни метров избыточна. Как уже отмечалось*, использование системы воздушного охлаждения для утилизации тепла, выделяемого ИТ- и сетевым оборудованием, накладывает некоторые ограничения на площадь машзала и соответственно на максимальную протяженность кабельного тракта в нем. Эта величина для типового машзала ЦОДа в среднем не превышает 72 м.

Во-вторых, унификация элементной базы безусловно уместна для ЦОДов, использующих модель colocation. Они рассчитаны на сдачу в аренду стойко-мест с обеспечением их гарантированным электроснабжением, соблюдением температурного режима и иных параметров окружающей среды. Фактически такие структуры представляют собой совокупность микро-ЦОДов, расположенных на одном архитектурном объекте. Для них характерно прямое подключение коммутаторов к соединительной линии телеком-оператора, в результате чего их количество соизмеримо с количеством стоек. В этом случае применение одномодовой оптики целиком и полностью оправдано хотя бы соображениями минимизации количества преобразований сигнала и связанного с ним падения надежности и некоторого увеличения задержки.

Для корпоративных ЦОДов ситуация меняется на прямо противоположную. В них суммарное количество соединительных линий и дополняющих их межзальных связей увеличенной протяженности в случае крупных объектов как минимум на порядок меньше общего количества стоек. В этой ситуации повсеместное применение одномодовой техники уже не столь очевидно и должно обосновываться отдельно.

Экономика многомодовых и одномодовых решений

Оставляя за кадром заметно большую эксплуатационную капризность одномодовой волоконной оптики по сравнению с многомодовой,

*А. Семенов. Ближайшие и среднесрочные перспективы развития СКС для ЦОДов. «ИКС» № 3'2023, с. 54.

примем в качестве постулата равенство их функциональных возможностей. Тогда вопрос о выборе типа элементной базы информационной проводки машинного зала переходит преимущественно в экономическую плоскость.

У профессиональных связистов, занимающихся волоконной оптикой, в ходу следующая интуитивно понятная формула:

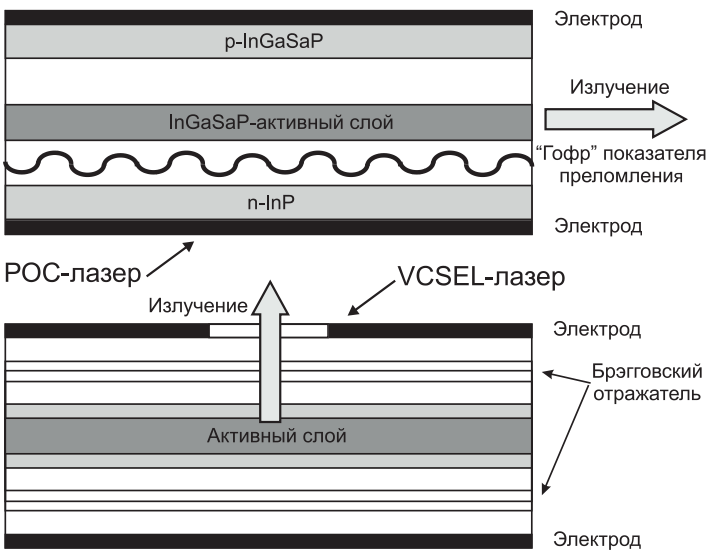
ВОЛП = ВОЛС + ВОСП,

означающая, что волоконно-оптическая линия передачи (ВОЛП) как технический объект представляет собой унитарную совокупность волоконно-оптической линии связи (ВОЛС), которая образует ее пассивную часть, и активного оборудования волоконно-оптической системы передачи (ВОСП). Каких-либо ограничений на область применения это соотношение не имеет, что позволяет привлечь его для анализа линий внутриобъектовой связи.

Заготовки одномодовых и многомодовых волокон формируются по одной и той же технологии, но в последнем случае за счет большей площади резко увеличивается расход дорогостоящих добавок, что сопровождается значительным удорожанием волокна. С другой стороны, стоимость оптических приемников и передатчиков определяют преимущественно фотодиод и лазер соответственно. Эта стоимость существенно увеличивается по мере перехода в длинноволновый рабочий диапазон, который характерен для одномодовой оптики.

Более того, сама технология изготовления VCSEL-лазера как излучателя «многомодового» окна прозрачности 850–950 нм заметно проще, чем РОС-лазера, применяемого в одномодовой технике (упрощенные структуры обоих лазеров показаны на рис. 1), что определяет больший выход годных.

Рис. 1. Упрощенная структура РОС- и VCSEL-лазеров ▼



Совокупное действие этих двух факторов обусловливает существование некоторой предельной протяженности кабельного тракта, при превышении которой следует безусловно строить линию связи на одномодовой элементной базе. Расчеты показывают, что этот предел составляет примерно 250 м, т.е. заметно превышает практически востребованный в машзале ЦОДа диапазон длин кабельных трактов. В комплексе это все означает, что многомодовые оптические линии имеют массовую область применения.

Многомодовые сетевые интерфейсы субтерабитного и терабитного диапазонов скоростей

О потенциальной востребованности многомодовой оптики для построения линий следующего поколения свидетельствует появление специализированных разработок нового скоростного диапазона.

В качестве примера сошлемся на опубликованный в начале 2023 г. документ Terabit BiDi MSA Technical Specification, который нормирует основные характеристики многомодовых сетевых интерфейсов 800G-SR4.2 и 1,6T-SR8.2. Примечательно, что таковые предлагаются сразу в двух вариантах дальности действия (см. таблицу): SR – стандартной и VR – малой (30–70 м в зависимости от категории используемого волокна). Последнее говорит о стремлении к оптимизации параметров сетевых интерфейсов для применения в условиях, когда задействуются много линий небольшой длины (как в машзале ЦОДа).

Сокращение предельной дальности действия сетевого интерфейса означает резкое уменьшение дисперсионного штрафа. Это как раз и открывает перспективы применения техники BiDi, которая из-за принятой в ней схемы формирования линейного сигнала предполагает использование более высоких тактовых частот, в результате чего изначально выдвигает повышенные требования в отношении дисперсионных параметров оптического тракта.

Из таблицы видно, что учет характерных для типовой области эксплуатации небольших длин кабельных трактов дает возможность ослабить требования к части параметров излучателя, применяемого в технике VR, и это положительно сказывается на стоимости решения.

Предполагается, что передача на скорости 800 Гбит/с осуществляется в соответствии со схемой Base8, а при переходе на следующий скоростной диапазон 1,6 Тбит/с используется схема Base16. В качестве разъема нормируется MPO/MTP, раскладка отдельных волокон и спектральных каналов по посадочным местам наконечника MPO12 и MPO16 схематически показана на рис. 2.

Хорошие экономические показатели интерфейсов BiDi обусловлены тем, что расстояние между оптическими несущими составляет 50 нм, т.е. увеличено в 1,5 раза по сравнению с системами SWDM. Это дает возможность существенно удешевить оптический фильтр и применять в интерфейсе излучатели с меньшей стабильностью центральной длины волны излучаемого света.

Новая разновидность многомодовых волокон

Перспективы внедрения экономически выгодных многомодовых интерфейсов BiDi следующего поколения можно существенно улучшить за счет применения в СКС машинного зала волоконно-оптических кабелей, световоды которых целенаправленно адаптированы для работы с данной разновидностью сетевой техники.

Речь идет о так называемых BiDi-волокнах с 50-микронной сердцевиной, которые разработаны на основе техники категории OM4. При прочих равных параметрах по спецификациям ANSI/TIA 492AAAF и IEC 60793-2-10 данные волокна отличаются от прототипа нормированием коэффициента широкополосности ΔF при лазерном возбуждении в первом окне прозрачности на двух длинах волн. Это не новинка, но с учетом предполагаемой области применения в качестве опорных использованы длины волн 850 и 910 нм, а не 850 и 953 нм, на которых осуществляется нормировка параметров волокон категории OM5. При всей внешней незаметности этого шага он существенно увеличивает выход годных в производстве, что положительно сказывается на отпускной цене продукции.

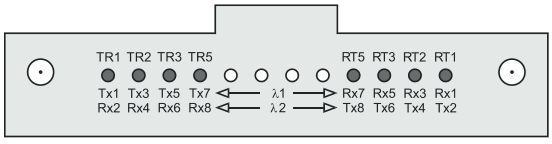
Функциональные возможности BiDi-волокон расширяются тем, что они изначально обратно совместимы по коэффициенту широкополосности с волокнами категории OM5 на опорных длинах волн. При этом для длины волны 910 нм, которая отсутствует в оригинальной спецификации прототипа, берутся значения из фирменных спецификаций, где принята его минимальная величина ΔF = 3100 МГц × км.

В настоящее время о возможности серийных поставок BiDi-волокон объявили две компании. Corning предлагает свою продукцию под торговыми марками OM3 HDR и OM4 HDR, а OFS Optics выпускает аналогичную технику как LaserWave Dual-Band (OM4+). Предельная дальность действия по кабелям с волокнами HDR и Dual-Band равна 100 м, что фактически в 1,5 раза превышает максимальную ожидаемую для реального ЦОДа величину.

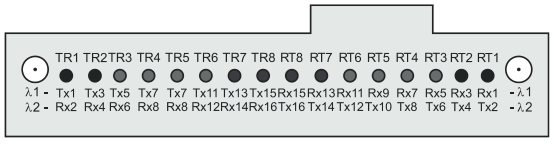
Тип интерфейса	800G-VR4.2 1,6T-VR8.2	800G-SR4.2 1,6T-SR8.2
Центральная длина волны, нм	842–868 900–916	844–863 900–915
Ширина линии излучения, нм	0,65 0,60	0,60 0,58
Мощность, вводимая в волокно, дБм	От 4 до -4,6	
Чувствительность приемника, дБм	-6,2	-6,4
Возвратные потери RL, не более, дБ	14	
Параметр Encircled Flux	Не менее 86 % при 19 мкм Не более 30% при 4,5 мкм	

▲ **Оптические параметры сетевых интерфейсов BiDi следующего поколения**

Отдельно укажем, что Corning обоснованно считает перспективными и бюджетные волокна OM3 HDR. Дело в том, что предельная протяженность кабельного тракта на этой технике составляет 80 м, что опять же превышает ожидаемый 70-метровый максимум. Этот запас определяется тем, что фирменные спецификации устанавливают для волокон OM3 HDR значение ΔF = 2890 МГц × км на длине волны 850 нм, что на 40% больше, чем для стандартного волокна категории OM3.



MPO12



MPO16

◀ **Рис. 2. Соответствие отдельных спектральных каналов посадочным местам вилки групповых наконечников MPO12 и MPO16**

Как мы видим, многомодовая волоконно-оптическая техника сохраняет свою актуальность в ЦОДах при скоростях передачи до 1,6 Тбит/с включительно, т.е. вопрос о ее полной замене на одномодовые решения отодвигается по меньшей мере до середины следующего десятилетия. Многомодовую линию передачи с указанным быстродействием предпочтительнее формировать на основе техники, которая целенаправленно разрабатывалась для этого скоростного диапазона. А появление специализированных сетевых интерфейсов и световодов для лазерной передачи субтерабитного и терабитного диапазонов скоростей в совокупности с готовностью промышленности к их серийному производству свидетельствует о высоком рыночном потенциале многомодовых волоконно-оптических решений для машзалов ЦОДов. ИКС

За что платим? Споры о длине витой пары в СКС и как их избежать

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

Заказчики порой настаивают на оплате только той длины витой пары, которая измерена тестером, и ни сантиметром больше. Подрядчики возражают: определенный метраж на объектах уходит в обрезки, это нужно учитывать. Кто прав? Как мерить и за что платить?

Приведем пример аргументации заказчика:

Результат прокладки слаботочного кабеля – соединение двух точек. Соответственно, работой является прокладка кабеля от точки до точки, что подтверждается кабельным журналом и результатами сертификационного тестирования. Все остальное – технология монтажа, которая заказчика не интересует.

Иногда для подкрепления позиции используются отсылки к другим сферам деятельности:

Для вязки арматурного каркаса по технологии раскладывается для резки и гибки больше арматуры, чем остается в изделии. Но к оплате принимается тоннаж готового каркаса, а не тот вес всей арматуры, которая использовалась. Отходы учитываются только в списании материала. В СКС должно быть так же!

Иногда заказчик даже может утверждать, что «данная методика определения объемов работ принята со всеми прочими подрядчиками на других объектах». Опыт автора показывает, что в сфере СКС это вовсе не так. Но давайте разберемся, какой метраж следует учитывать и почему. Начнем с того, какая бывает длина и как ее можно измерить.

Длина физическая и электрическая

Все ограничения по длине, записанные в стандартах, касаются **физической длины, определяемой по меткам на оболочке кабеля**. В момент прокладки это единственный ориентир для монтажников. Измерения прибором будут проводиться позже, а отрезать кабель нужно здесь и сейчас.

Ответственность производителей витой пары – обеспечить, чтобы метки длины на оболочке кабеля были честными. Опыт показывает, что в подавляющем большинстве случаев так оно и есть, причем как для признанных брендов, еще несколько лет назад широко представленных на нашем рынке, так и для заместивших их китайских и отечественно-китайских производителей. В этом есть своя логика. Если производитель ошибется в меньшую сторону и поставит метки длины слишком часто, его тут же обвинят в «обвешивании покупателя», что чревато потерей репутации раз и навсегда. Проверить точность меток может любой клиент с помощью обычной рулетки. С другой стороны, если располагать метки дальше друг от друга, чем 1 м, то это ведет к убыткам. Каждый лишний сантиметр для коробки 305 м вызывает перерасход более 3 м кабеля, для катушки 500 м – 5 м, а на производстве выпускаются многие тысячи таких упаковок. Подобные неточности негативно сказываются на экономических показателях производства, изготовителю это невыгодно. Проще намеренно заложить в упаковку пару лишних метров кабеля, чтобы обезопасить себя от возможных обвинений в «недовесе», но при этом точно отмерять физические расстояния и иметь возможность точно просчитывать все параметры производства.

На сегодняшний день риск столкнуться с неверной физической маркировкой длины невелик. Метки на оболочку наносятся автоматическим оборудованием; отладить и контролировать процесс технически не сложно. Однако возникает вопрос точности определения физической длины монтажниками. Обычно за погрешность измерения принимают 1/2 цены деления шкалы. В нашем случае шкала формируется метками, отстоящими друг от друга на 1 м, и можно было бы сказать, что на каждом конце сегмента погрешность составляет ±0,5 м, а для сегмента в целом ±1 м. Однако так происходило бы, если бы взору были доступны оба деления шкалы. На объекте же монтажник ориентируется только на ту метку, которую видит, а заканчиваться кабель может на расстоянии до 1 м от нее, там, где другой метки уже нет. И так на обоих концах. В итоге имеет место погрешность в сторону увеличения, и в сегменте она может достигать 2 м. Для постоянной линии длиной около максимально допустимых 90 м это немного – чуть больше 2%. Но ес-

ли сегмент короткий, длиной 20 м или даже 15 м (короче которых в обычных СКС ставить не рекомендуется), то погрешность составит уже 10–13%. При этом любой практикующий монтажник знает, что в случае сомнений ошибаться надо в большую сторону. Лишний кабель всегда можно обрезать при заделке. Если же метража не хватит, придется перепротягивать сегмент заново.

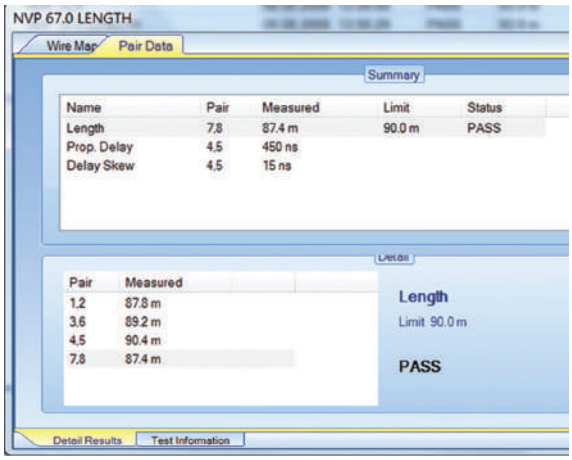
Приборы измеряют **электрическую длину**. Точнее, **приборы измеряют время** Δt, за которое сигнал проходит от ближнего конца сегмента до дальнего и обратно, а затем **вычисляют длину** через этот временной промежуток и заданную в памяти прибора номинальную скорость распространения сигнала NVP (Nominal Velocity of Propagation), выраженную в процентах от скорости света в вакууме.

$$L_{сегмента} = NVP / 100 \cdot c \cdot \Delta t / 2$$

Типовые значения NVP для витой пары категорий 5e и 6 лежат в диапазоне от 67 до 72%. Для кабелей категории 6A с плотным повивом пар NVP может составлять 65%, а у кабелей с индивидуальным экранированием пар это значение может достигать 78–80% независимо от заявленной категории.

Электрическая длина не всегда совпадает с физической. Расхождение есть хотя бы потому, что шаг повива у каждой пары в кабеле свой. Электромагнитная волна в туго сплетенной паре распространяется медленнее, чем в паре со слабым повивом. Для каждого четырехпарного кабеля тестеры выводят четыре значения электрической длины, и расхождение между парами при предельно допустимой длине постоянной линии 90 м может составлять несколько метров. Длиной кабеля считается наименьшее значение из четырех, но даже оно совпадает с физической длиной не всегда. Это легко проиллюстрировать на конкретном примере.

Из заводской коробки был отмотан участок кабеля категории 5e с заявленным производителем значением NVP = 67%. Начальная видимая метка длины 17098 м, конечная 17188 м. Поскольку кабель обрезан и заделан на модули сразу после видимых меток, его физическая длина составляет 90 м с точностью до нескольких сантиметров. На рисунке показаны результаты измерения длины прибором сертификационного класса с адаптерами постоянной линии и установленным значением NVP = 67,0%. Метраж адаптеров исключен из результатов программным обеспечением прибора, выводится только собственная длина постоянной линии. Расхождение налицо: измеренная электрическая длина составила 87,4 м вместо ожидаемых 90 м.



◀ Результаты измерения электрической длины четырехпарного кабеля, физическая длина которого составляет 90 м

Либо значение NVP задано производителем неточно, либо прибор неточно измеряет время (а значит, и рассчитывает длину). А может быть, и то и другое. Второй параметр легко проверяется по техническим спецификациям приборов, публикуемым их изготовителями в открытом доступе. Сопоставим данные о точности для нескольких марок тестеров, встречающихся на территории России (табл. 1 и 2).

Табл. 1. Точность измерения электрической длины кабеля сертификационными тестерами Fluke DTX-1800 и DSX(2)-8000 ▼

	Только основной модуль, измерение по отражению от дальнего конца	Основной и удаленный модули на концах сегмента
Максимальное расстояние, измеряемое в среде витой пары, м	800	150
Разрешающая способность	0,1 м или 1 фут	0,1 м или 1 фут
Точность	± (0,3 м + 2%) для расстояний от 0 до 150 м ± (0,3 м + 4%) для расстояний от 151 до 800 м	± (0,3 м + 2%)

По приведенным данным, для 90-метрового сегмента точность измерения длины составит ±2,1 м (2,3%). Для сегмента длиной 15 м погрешность больше – 4% (±0,6 м). Нужно отметить, что заявленная производителем разрешающая способность по времени (1 нс) кратно ухудшается заявленной точностью измерения задержек распространения ± (2 нс + 2%) для всех упомянутых выше диапазонов расстояний. Одна наносекунда – лишь минимальный шаг по времени, используемый прибором в вычислениях. Допуски

Табл. 2. Точность измерения электрической длины кабеля сертификационным тестером AEM CV100 ▼

	Функция тестирования длинных сегментов	Основной и удаленный модули на концах сегмента
Максимальное расстояние, измеряемое в среде витой пары, м	1000	600
Разрешающая способность	0,1 м	0,1 м
Точность	± (1 м + 4%) от 0 до 1000 м	

же при измерении временных интервалов в нашем примере составляют 11 нс для сегмента 90м и округленно 4 нс для сегмента 15 м.

Заявленную разрешающую способность по длине 0,1 м тоже следует воспринимать не как точность, а как минимальную цену деления, предусмотренную в приборе. Особенно если учесть, что переход на систему мер, принятую в США и некоторых других странах мира, увеличивает минимальный шаг до 1 фута – а значит, выводимые результаты огрубляются сразу втрое.

Схожие показатели заявляет и другой производитель сертификационных тестеров (табл. 2).

Спецификации на приборы Softing WireXpert последних моделей декларируют точность измерения длины в медных средах ±0,5 м для любых расстояний от 0 до 500 м. Для семейства LanTEK IV его производитель, Trend Networks, заявляет в спецификациях только разрешающую способность 0,1 м в диапазоне от 0 до 600 м, но не говорит о точности. Отсутствие процентного допуска или скупость открытых технических данных намекает на не самую высокую точность измерений.

Сертификационные тестеры совершенствуются, и было бы логично ожидать, что погрешность приборов уменьшается от поколения к поколению. Однако фактические данные говорят о том, что точность измерения засечек времени мало меняется не только год от года, но даже от класса к классу измерительных устройств. В России на руках у монтажников осталось много карманных тестеров Microscanner2 (а некоторые помнят и его предшественника, Microscanner первого поколения) – эти приборы на порядок проще и дешевле, чем сертификационные тестеры. Но даже у Microscanner2 при диапазоне измерений до 460 м заявлена похожая разрешающая способность 0,3 м (1 фут) и принципиально схожая точность ±4% или 0,6 м (2 фута) в зависимости от того, что больше. В измерениях длины сертификационные приборы не достигли особого прогресса в сравнении с тестерами схемы разводки.

В измерениях длины сертификационные приборы не достигли особого прогресса в сравнении с тестерами схемы разводки

В идеале измеренная электрическая длина должна совпадать с физической длиной. Но по приведенным выше причинам, даже если величина NVP задана производителем верно, все равно погрешность в измерении времени приборами приведет к разбросу значений длины порядка 4%.

Точность, с которой задано значение скорости NVP

Стандарт ANSI/TIA/EIA-568-B.1, действовавший в начале 2000-х гг., предусматривал допуск ±10% для величины NVP, задаваемой производителями кабеля. Версия B стандартов давно вышла из употребления – ее последовательно сменили версии C, D и даже E различных стандартов TIA. Что интересно, в них допуск ±10% уже не упоминается. Чтобы на него выйти, нужно отслеживать нормативные документы в обратном хронологическом порядке вплоть до версии B. И даже в стандарте TIA-1152 [A], задающем требования к полевым тестерам и измерениям в СКС на основе витой пары (Requirements for Field Test Instruments and Measurements for Balanced Twisted-Pair Cabling), ни в 2009 г., ни в 2016 г. этот допуск не упоминался. Приводятся только ссылки на стандарты, которые сами ссылаются на предшествующие стандарты, и т.д. Этот бюрократический казус неоднократно обсуждался на отечественных и зарубежных форумах и площадках. Однако среди технических специалистов допуск ±10% для NVP считается настолько общим местом, что отсутствие его упоминания в тексте современных стандартов никого не смущает. Более того, этот допуск в явном виде указан в нашем ГОСТ Р 53245-2008, а его на территории России никто не отменял. В тексте четко прослеживается происхождение от стандарта ANSI/TIA/EIA-568-B.1 (безотносительно качества перевода с английского языка) – достаточно просто сопоставить фрагменты с соответствующими пунктами нашего ГОСТ Р (табл. 3).

В принципе поправку на неопределенность NVP можно указывать как +10%, а не ±10%. Минус можно опустить, поскольку при погрешности в меньшую сторону результаты измерения длины заведомо попадут в допустимый стандартом максимальный предел 90 м для постоянной линии или 100 м для канала. Минимальный же предел (расстояние не менее 15 м для постоянной линии) имеет рекомендательный характер, и его несоблюдение к появлению результата Fail не приводит.

Чтобы проиллюстрировать важность правильного указания NVP в настройках прибора, можно снова обратиться к уже приводившемуся примеру с участком кабеля категории 5e. Для сравнения на нем были выполнены измерения сертификационным тестером не только со значением NVP = 67,0%, заявленным производителем, но и со значениями 72,0% и 80,0% (табл. 4).

Самая короткая (слабо сплетенная) пара в образце – коричневая, поэтому во всех измерениях общая длина кабеля определяется по ней. Погрешность рассчитывалась относительно физической длины 90 м.

Несмотря на то что уже при NVP = 72% длина превысила допустимые 90 м, сертификационный тестер показал результат Pass для постоянной линии, поскольку погрешность не превысила допустимых 10% для самой короткой пары. Результат Fail прибор показал только при NVP = 80%, и погрешность в этом случае составила уже более 15%.

ANSI/TIA/EIA-568-B.1	ГОСТ Р 53245-2008
Commercial Building Telecommunications Cabling Standard Part 1: General Requirements	**Информационные технологии Системы кабельные структурированные Монтаж основных узлов системы Методы испытания**
11.2.4.3 Length	3.1.3.3 Длина
11.2.4.3.1 Physical length vs. electrical length	
The physical length of the permanent link/channel is the sum of the physical lengths of the cables between the two end points. Physical length of the permanent link/channel may be determined by physically measuring the length(s) of the cable(s), determined from the length markings on the cable(s), when present, or estimated from the electrical length measurement. The electrical length is derived from the propagation delay of signals and depends on the construction and material properties of the cable (see ANSI/TIA/EIA-568-B.2)	Физическая длина постоянной линии или канала представляет собой сумму физических длин кабелей, соединяющих две конечные точки. Физическая длина может быть определена: – механическим измерением длины кабелей по внешней оболочке с помощью инструмента для измерения длины; – расчетом длины кабелей на основании меток длины, нанесенных на их внешние оболочки; – оценкой длины кабелей на основании измерения электрической длины. Электрическую длину линии рассчитывают измерительным прибором с учетом времени распространения сигнала в линии, и она зависит от конструкции (шаг повива) и свойств материала кабеля (диэлектрическая постоянная)
When physical length is determined from electrical length, the physical length of the link calculated using the pair with the shortest electrical delay shall be reported and used for making the Pass or Fail decision. The Pass or Fail criteria is based on the maximum length allowed for the channel or permanent link given in figures 11-1 and 11-2 plus the **nominal velocity of propagation (NVP) uncertainty of 10 percent**	При оценке физической длины на основании результата измерения «электрической» длины линии расчет проводят для пары с самым коротким временем распространения, обычно используемой для индикации результатов полевого тестирования и для критерия Pass/Fail. Критерий Pass/Fail основан на максимально допустимой длине канала или постоянной линии (рисунки 1 и 2) и допущении **неопределенности номинальной скорости распространения (NVP) в 10%**
NOTE – Calibration of NVP is critical to the accuracy of length measurements (see ANSI/TIA/EIA-568-B.2)	При полевом тестировании длины канала или постоянной линии в полевом тестере должно быть установлено значение номинальной скорости распространения сигнала (Nominal Velocity of Propagation, NVP), соответствующее виду кабеля, проходящего тестирование. Правильная калибровка параметра NVP в полевом тестере является необходимым условием точного измерения электрической длины

▲ Табл. 3. Сопоставление стандарта ANSI/TIA/EIA-568-B.1 и ГОСТ Р 53245-2008

С использованным для экспериментов образцом прибор начинает выдавать результат Fail при электрической длине коричневой пары (а значит, и кабеля) 99 м – ее можно получить при NVP = 75,9%. Необходимо помнить, что допуск ±10% означает не проценты от скорости света в вакууме, а ±10% от самого значения NVP, выраженного в процентах. Для кабеля с реальным NVP = 67% допустимыми будут не значения от 57 до 77%, а более узкий диапазон от 60,3 до 73,7%.

Примечательно расхождение между упомянутыми выше граничными значениями NVP 75,9% и 73,7%. Причина в том, что образец, на котором проводились измерения, на самом деле не соответствует заявленной производителем номинальной скорости распространения 67%. Весьма вероятно, что фактическое значение NVP для этого кабеля составляет ~69%. Но как в полевых условиях отличить неточность измерения времени (по вине прибора) от неточности задания NVP производителем? Никак. Поэтому и допуски такие широкие.

Для сопоставления на том же образце были выполнены измерения тестером Microscanner2 (табл. 5). В нем нельзя указать десятые доли NVP – только целочисленные значения. Прибор не умеет вычитать длину шнуров, которыми его подключают к тестируемому сегменту, – это нужно считать вручную, заново измеряя длину шнуров при каждой смене величины NVP в настройках. И в нем не применяется критерий Pass/Fail. Однако результат измерений длины по парам при заданном значении NVP = 67% оказался ближе к физической длине кабеля, чем у сертификационного тестера!

Табл. 4. Измерения кабеля сертификационным тестером ▼

NVP, %	**67,0**	**72,0**	**80,0**
Синяя пара, м	90,4	97,1	107,9
Оранжевая пара, м	87,8	94,3	104,8
Зеленая пара, м	89,2	95,8	106,5
Коричневая пара, м	87,4	93,9	104,3
Электрическая длина кабеля, м	**87,4**	**93,9**	**104,3**
Физическая длина кабеля, м	90	90	90
Расхождение, м	-2,6 (длина занижена)	3,9	14,3
Погрешность, %	2,89	4,33	15,89
Критерий Pass/Fail	PASS	PASS	FAIL

NVP, %	67	72	80
Длина шнуров, м	2 x 1,7 = 3,4	2 x 1,8 = 3,6	2 x 2,0 = 4,0
Синяя пара, м	95,1	102,2	113,5
Оранжевая пара, м	92,2	99,1	110,0
Зеленая пара, м	93,9	100,9	112,0
Коричневая пара, м	92,0	98,9	109,9
Электрическая длина кабеля за вычетом шнуров, м	**88,6**	**95,3**	**105,9**
Физическая длина кабеля, м	90	90	90
Расхождение, м	-1,4 (**длина занижена**)	5,3	15,9
Погрешность, %	1,56	5,89	17,67

▲ Табл. 5. Измерение кабеля карманным тестером с функцией измерения длины

Разумеется, изготовители кабеля стараются указывать NVP точно – это в их интересах. Но на кабельных заводах постоянно ведутся эксперименты с разными шагами повива, сочетаниями пар, с медной катанкой от разных поставщиков, разными диаметрами проводников, типами и толщинами изоляции для них, и так далее в меру фантазии и технических возможностей производителя. Расхождения в NVP от партии к партии продукции возможны и даже ожидаемы. Потому в свое время и появился допуск ±10%. Опытных монтажников такой разброс не смущает – они на практике знают, что если соблюдать ограничение для физической длины постоянной линии 90 м (и 100 м для канала), то измерения по электрической длине всегда дадут результат Pass. Даже если величина NVP заявлена производителем не совсем точно, а приборы замеряют время со значимой погрешностью.

Сколько кабеля уходит в обрезки

Как бы ни был детально проработан проект и выполнены чертежи, при протяжке кабеля идеально точно угадать с длиной невозможно. Монтажники оставляют «хвосты» в 0,5–1 м со стороны рабочего места и 1–1,5–2 м со стороны телекоммуникационного помещения. Это не запас 0,3 м (1 фут) и 3 м соответственно, который стандарты рекомендуют оставлять на будущие потребности в перезаделке и локальных изменениях. Запас укладывается в трассах, он предусматривается еще на стадии проектирования. Его метраж может и должен входить в результаты измерений. Монтажники же при протяжке закладываются на неточности в проекте – шкаф может располагаться не совсем так, как указано на чертеже, или патч-панель в нем может занимать не ту позицию, которая предполагалась изначально, и метраж при прокладке кабеля по трассам может несколько отличаться. Кабель нужно обрезать по месту. Значит, протягивать придется с запасом, и расход на обрезки неизбежен. При средней длине сегмента ~50 м пара метров, срезанных на концах, даст расход не менее 4%. Плюс еще какой-то метраж останется в коробке или на катушке, когда кабель на ней будет заканчиваться. Бывают объекты с «неудобными» расстояниями, из-за которых в упаковке остается 20–25 м кабеля, которые некуда «пристроить».

Многие монтажные компании при работе записывают метки длины при отметке и протяжке кабеля. Это позволяет точно знать, сколько кабеля осталось в каждой упаковке, и использовать его более экономно, минимизируя остатки. Но даже при таком подходе свести обрезки к нулю в принципе невозможно. Практика показывает, что в среднем по разным объектам на обрезки уходит примерно 10% метража. На «неудобных» объектах случается и 15%. А когда в проект по ходу исполнения постоянно вносятся уточняющие изменения, расход на обрезки может оказаться еще больше.

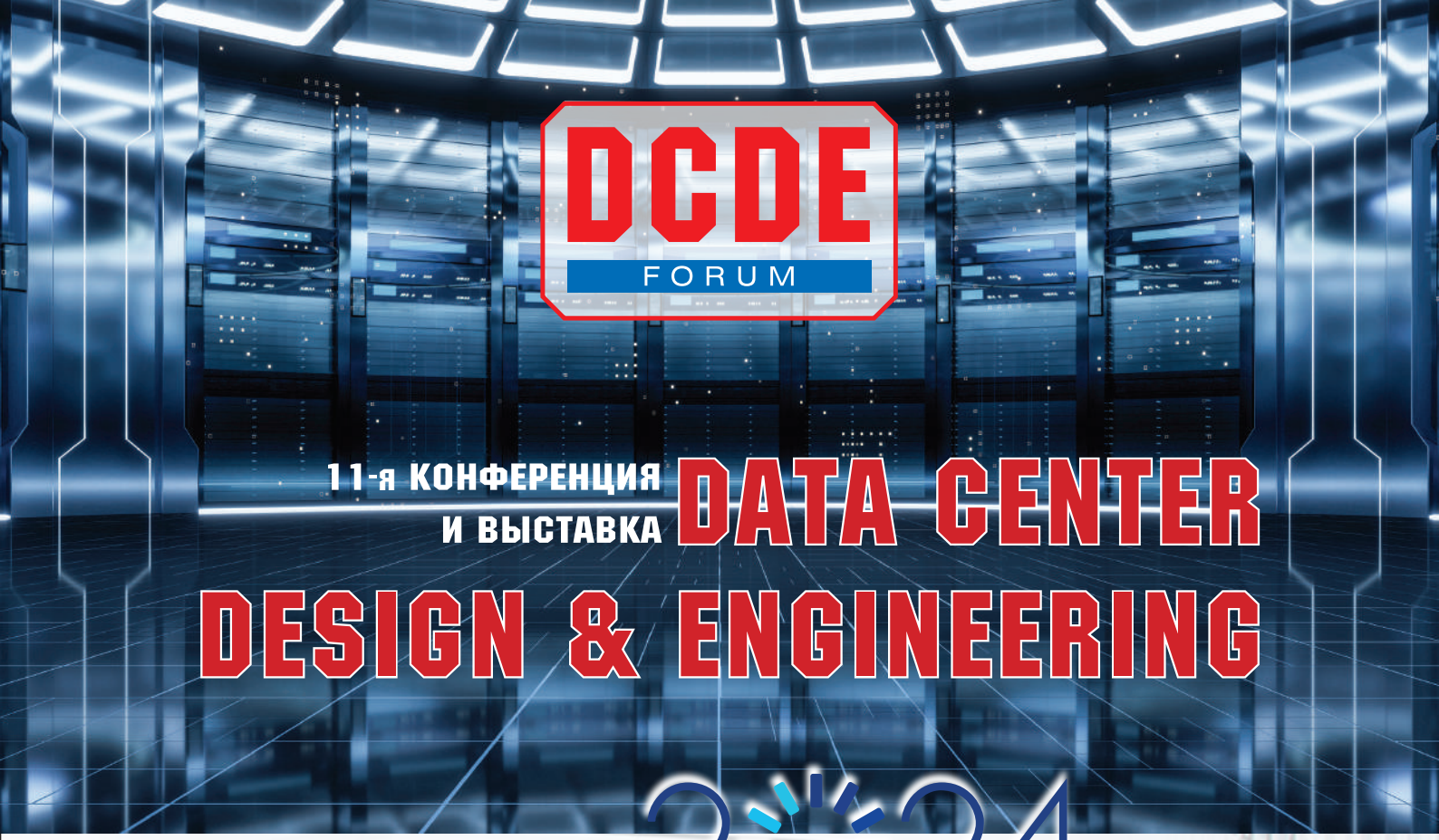
Как избежать споров

Чтобы с заказчиками реже возникали разногласия, подобные тем, что описаны в начале статьи, необходимо, чтобы все осознавали разницу между физической и электрической длиной. Измерения всегда имеют погрешность, и в данном случае она довольно велика.

Кроме того, определенный процент на обрезки нужно в явном виде закладывать в договор, давая необходимые пояснения заказчику на этапе переговоров, до заключения соглашения, а не после. Типовая цифра составляет 10%. В большинстве случаев длина, просуммированная по результатам сертификационных измерений, плюс 10% на обрезки соответствуют действительному расходу кабеля.

Обрезки учитываются не только в списании материала, но и в трудозатратах. Какая-то длина срезана, но весь этот кабель отматывали, затягивали в трассы, перемещали и укладывали. С этим метражом проводились работы, и они должны быть оплачены.

Если изначально в смету было заложено слишком много кабеля, то нетронутые упаковки могут остаться заказчику как оплаченный им материал, а в расчете стоимости работ этот метраж не учитывается. Но опытные подрядчики способны довольно точно просчитывать проекты, если потребности заказчика сформулированы внятно и необходимая информация по объекту доступна. Тем не менее во избежание споров все подобные нюансы нужно предусмотреть и в явном виде указать в договоре, а затем просто выполнять его положения. ИКС



11-я КОНФЕРЕНЦИЯ И ВЫСТАВКА DATA CENTER DESIGN & ENGINEERING

21 мая 2024

Москва, Holiday Inn Moscow Sokolniki

Рынок инженерных систем ЦОДов находится в стадии серьезной трансформации. Кардинально меняется состав поставщиков технических решений, новые продукты требуют более тщательных проверок, тестирования, зачастую меняются архитектуры решений и выбор технологий. И это все происходит на фоне развития отрасли: масштаб и количество крупных ЦОДов увеличиваются, активно создаются дата-центры в регионах.

Фокус DCDE-2024

- Отечественные решения для инженерной инфраструктуры
- Префабы, модули и контейнерные ЦОДы
- Системы электропитания и охлаждения
- Инженерная инфраструктура для систем ИИ
- Наилучшие практики эксплуатации

подробно о программе и участниках на сайте конференции dcdeforum.ru

За дополнительной информацией обращайтесь

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

Облачные библиотекари и российский рынок DBaaS

Николай Носов

Использование единой платформы для работы с данными становится необходимостью, и популярность облачных баз данных на российском рынке растет. В условиях санкций ставка делается на решения open source.

От наскальных рисунков до библиотек

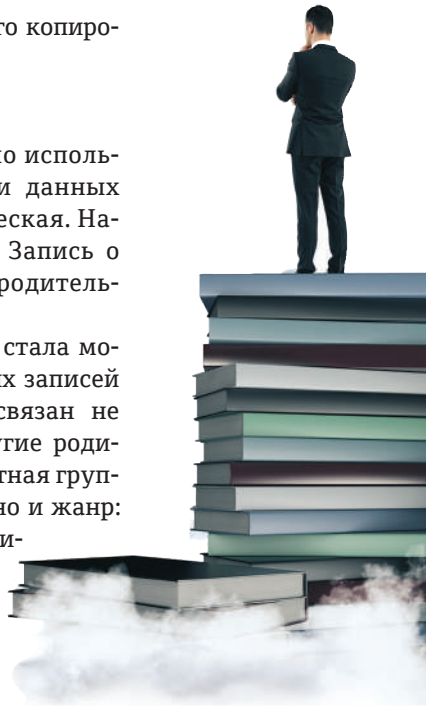
Развитие человечества невозможно без технологий хранения информации, обеспечивающих передачу знаний, опыта, норм поведения и морали. Поверхности скал с рисунками бушменов, глиняные таблички с клинописью шумеров, папирусные свитки Александрийской библиотеки, переписываемые тибетскими монахами манускрипты, печатные научные журналы – все это сменяющие друг друга носители информации. Проблема поиска нужных данных возникла еще до информационной эры. Путем простого перебора трудно найти книгу даже в шкафу, не говоря уж о библиотеке. Лучше упорядочить книги, например, по фамилии автора, чтобы у каждой было место на конкретной полке, в конкретном шкафу, в конкретном зале, а искать по каталогу с карточками, на которых указано физическое расположение объекта поиска. И уже по такой карточке книгу найдет и выдаст специально обученный человек – библиотекарь, который также отвечает за расстановку книг в нужном порядке и ведение каталога.

Компьютерная революция перенесла информацию в цифру. Объемы данных колоссально увеличились и продолжают расти, на «новой нефти» строятся бизнесы компаний и экономики стран. Цифровые записи надо собирать в базах данных (БД), хранить, предоставлять для дальнейшего анализа. Ими надо управлять, и для этого на смену библиотекарям пришли системы управления базами данных (СУБД).

СУБД позволяет «ставить книгу на полку», создавать для нее «карточку», проводить поиск, выдавать и «отправлять в макулатуру». Говоря современным языком: размещать, перемещать, читать и удалять данные. Как правило, СУБД – это сложное программное обеспечение, включающее языки запросов, описания и обработки данных. В состав решений входят системы управления транзакциями, резервного копирования и восстановления.

Модели организации данных

СУБД можно классифицировать по используемой в них модели организации данных (табл. 1). Самая простая – иерархическая. Например: страна – область – город. Запись о стране в такой системе называется родительской.



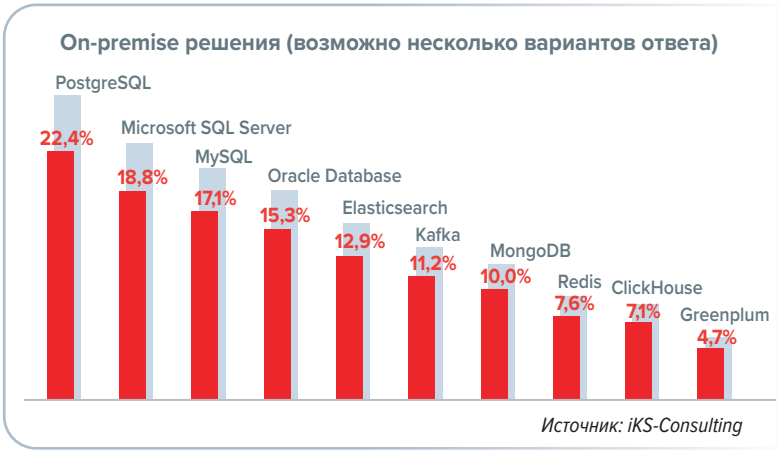
Развитием иерархической модели стала модель сетевая, в которой родительских записей несколько. Скажем, с человеком связан не только адрес проживания, но и другие родительские записи – профессия, возрастная группа. А у книги есть не только автор, но и жанр: компьютерные технологии, путеводители, беллетристика. Примером СУБД с такой организацией данных может служить разработанная еще в 1970-х гг. Integrated Database Management System (IDMS).

В реляционных БД данные хранятся в таблицах с определенными связями между ними. Например, у таблицы с жильцами дома есть связи с таблицами профессий и возрастных групп. Реляционные БД делятся на базы с хранением по строкам (PostgreSQL) и по столбцам (ClickHouse, Vertica). Колоночные (с хранением по столбцам) базы лучше подходят для аналитических операций, в то время как для транзакционных нагрузок предпочтительнее базы, ориентированные на строки. СУБД различаются и по области применения. Например, СУБД Greenplum (основанная на PostgreSQL) предназначена для параллельной обработки и работы с Big Data.

Среди других моделей организации данных стоит выделить документоориентированные, объектно ориентированные, графовые, «ключ – значение». В модели «ключ – значение» данные

Табл. 1. Классификация СУБД по типу организации данных ▼

Модель	Организация данных	Примеры СУБД
Иерархическая	Данные организованы в виде иерархии, где каждый элемент имеет родительский элемент и может иметь один или нескольких дочерних элементов	IMS (Information Management System) от IBM
Сетевая (Network Database)	Каждая запись может иметь несколько родительских записей и несколько дочерних записей, что позволяет представлять сложные связи между данными	IDMS
Реляционная	Данные организованы в виде набора взаимосвязанных таблиц	MySQL, Oracle Database, Microsoft SQL Server, PostgreSQL, ClickHouse, Greenplum
«Ключ – значение» (Key – Value)	Данные хранятся в виде пар «ключ – значение»	Redis
Объектно ориентированная	Данные представлены в виде объектов	Db4o, Versant
Документоориентированная	Для хранения и обработки документов в форматах, например, JSON или XML	Elasticsearch, MongoDB
Графовая	Данные представлены в виде графа, где каждый элемент представляет собой узел, а связи между элементами – ребра	Amazon Neptune, Neo4j



▲ Рис. 1. Использование различных СУБД в России, 2023 г.

хранятся в виде пар, где ключи являются строками, а значения могут быть строками, списками или множествами. По ключу производится получение, установка, обновление и удаление элементов. Модель обеспечивает высокую производительность, что важно для приложений, использующих кэширование, очереди сообщений и аналитику в реальном времени.

На российском рынке наиболее популярна реляционная модель. По данным исследования, проведенного в конце 2023 г. аналитическим агентством iKS-Consulting, чаще всего применяются следующие СУБД: PostgreSQL (ее используют 22,4% опрошенных), Microsoft SQL Server (18,8%), MySQL (17,1%) и Oracle Database (15,3%).

Заметную долю имеют СУБД документоориентированных моделей: Elasticsearch (12,9%) и MongoDB (10%). Данные хранятся в форматах JSON (Elasticsearch) и BJSON (MongoDB). СУБД Redis (модель «ключ – значение») эксплуатируют 7,6% опрошенных.

Специфической системой управления данными является распределенный брокер сообщений Kafka (11,2%). В используемой потоковой модели (она же publish – subscribe, т.е. «публикация – подписка») данные отправляются в «топики» (topics), откуда могут быть прочитаны несколькими «подписчиками» (subscribers). Каждый подписчик может читать данные из топика независимо от других подписчиков, что обеспечивает масштабируемость и отказоустойчивость системы.

DBaaS: плюсы и минусы

Накопление данных и управление ими – большой труд, зачастую непрофильный. Неудивительно, что его давно стали отдавать на аутсорсинг – сначала в монастыри и библиотеки, а в цифровой век – в облако, где в базах данных собираются данные, управление которыми осуществляется по модели DBaaS (Database as a Service).

Использование DBaaS имеет преимущества, свойственные всем облачным сервисам:

- Упрощение управления базой данных. Задачи установки, настройки и обслуживания перекладываются на поставщика услуг, что дает организациям возможность сосредоточиться на основной деятельности, не тратя время и ресурсы на управление БД.
- Масштабируемость и гибкость. DBaaS позволяет легко увеличивать или уменьшать ресурсы БД в зависимости от потребностей, экономя на инфраструктуре для пиковых нагрузок.
- Автоматическое обновление. Провайдеры анализируют обновления СУБД и устанавливают их, гарантируя организациям доступ к новейшим функциям.

Табл. 2. Характеристики DBaaS ▼

Характеристика	Плюсы	Минусы
Стоимость владения	Экономия средств в краткосрочной перспективе. Не нужны инвестиции в инфраструктуру, оборудование и лицензии на ПО. Организации снижают накладные расходы на ИТ, перекладывая рутинные задачи сопровождения БД на поставщика услуг. Оплачиваются только используемые ресурсы БД	Долгосрочные затраты. По мере увеличения размера и времени использования базы данных затраты, связанные с DBaaS, могут значительно возрасти. Организации должны тщательно анализировать свои модели использования и ценообразование, предлагаемое поставщиком. Часто при длительном использовании сервиса on-premise-решение становится экономически более выгодным
Доступность, надежность, контролируемость	Поставщики DBaaS обеспечивают высокую доступность благодаря использованию надежных дата-центров, автоматического резервного копирования, аварийного восстановления и сервисов репликации	Отсутствие контроля над базовой инфраструктурой и конфигурацией БД может быть недостатком для организаций, которым нужна кастомизированная настройка или которые предъявляют строгие требования к безопасности. Также компании зависят от поставщика услуг в обслуживании и управлении БД, что может быть критичным при простоях провайдера или проблемах с качеством обслуживания
Производительность	Поставщики DBaaS часто оптимизируют свою инфраструктуру и конфигурации баз данных для обеспечения высокой производительности	Облачный сервис может уступать по производительности БД на выделенной инфраструктуре. Общий характер базовой инфраструктуры может приводить к колебаниям производительности, особенно в периоды пикового использования
Безопасность данных	Облачные провайдеры, как правило, имеют более квалифицированных специалистов по информационной безопасности, чем заказчики, и могут повысить защищенность решений	Хранение конфиденциальных данных в облачной системе вызывает опасения по поводу безопасности и конфиденциальности. Организациям необходимо тщательно оценить меры безопасности, применяемые поставщиком услуг, и проверить выполнение требований регуляторов

«База данных – фундамент для любых приложений, – отмечает Владимир Шульга, заместитель генерального директора и руководитель блока продуктовой разработки Cloud.ru. – Услуга DBaaS позволяет разворачивать базу за считанные минуты, экономя заказчику время, средства и ресурсы. Клиент быстро получает готовые экземпляры базы данных с известной производительностью и надежностью, и при этом ему не требуется большая команда специалистов».

Однако идеальных решений на все случаи жизни не существует. Некоторые характеристики DBaaS могут обернуться как достоинствами, так и недостатками (табл. 2).

Кроме того, при использовании облачных решений заказчики могут столкнуться с трудностями при переносе своих данных и приложений к другому поставщику DBaaS или на собственную площадку.

DBaaS и импортозамещение

Уход западных вендоров, перенос систем в отечественные облака и появление новых, недостаточно проверенных решений породили проблемы, специфичные для российского рынка. Это прежде всего выбор из оставшихся на рынке поставщиков сервисных услуг и решений, а также интеграция облачных СУБД в уже имеющиеся у заказчика системы. «Для эффективного развития рынка DBaaS нужна стандартизация подходов к работе с управляемыми сервисами. Это касается, в частности, вопросов информационной безопасности, для которых облачные платформы разрабатывают собственные рекомендации и стандарты. Компании стали использовать новые продукты и, следовательно, чаще сталкиваются с разрозненностью технологического стека. Бизнесу нужны новые интеграции между сервисами и экспертиза для их настройки», – подчеркнул Всеволод Грабельников, руководитель по развитию группы сервисов платформы данных компании «Яндекс».

Уход западных вендоров повысил спрос на облачные базы данных российских провайдеров. «В марте 2022 г. количество пользователей облачных баз данных Selectel увеличилось на 25% по сравнению с февралем 2022 г. и на 250% – по сравнению с мартом 2021-го, – говорит Александр Гришин, менеджер DBaaS-продуктов компании Selectel. – А по итогам 2022 г. выручка Selectel в сегменте DBaaS выросла более чем втрое».

Подстегивает спрос на DBaaS-сервисы и усиливающийся в течение последних лет тренд к переходу с проприетарного ПО на open source-решения, например переход с СУБД Oracle или Microsoft SQL Server на PostgreSQL или с Elasticsearch на Opensearch. В ответ на запросы рынка провайдеры DBaaS расширяют свой портфель решений за счет СУБД с открытым исходным кодом.

Чаще всего российские СУБД основаны на open source-решении PostgreSQL. Это, в частности, внесенные в Единый реестр российских программ для ЭВМ и баз данных (ЕРРП) Postgres Pro, ADPG, Jatoba, «Квант-Гибрид», Proxima BD. На Greenplum основаны SDP AnalyticDB, Arenadata DB, Data Ocean.Analytical WareHouse (табл. 3).

Однако по модели DBaaS приведенные в таблице решения почти не предлагаются. Российские облачные провайдеры DBaaS, как правило, предоставляют проприетарные СУБД западных вендоров (Oracle Database, Microsoft SQL Server), свои разработки (ClickHouse компании «Яндекс») или решения open source, самостоятельно обеспечивая их поддержку. Среди крупных российских облачных провайдеров проприетарное российское решение (Postgres Pro) удалось обнаружить только у VK.

Кому выгодно?

Сервис DBaaS интересен прежде всего компаниям, уже использующим облачные вычисления и хранящим данные в облаках. Например, в рамках сервиса Yandex Cloud с 2019 г. внешним пользователям доступна разработанная «Яндексом» открытая распределенная SQL-база данных YDB. Наличие этой СУБД помогло «Яндексу» с большим отрывом выйти в лидеры на российском рынке DBaaS (рис. 2).

Активнее всего потребляют сервисы платформы данных «Яндекса» банки, ритейл и ИТ-ком-

Табл. 3. Российские реляционные СУБД, включенные в ЕРРП ▼

Open source-прототип	СУБД	Дата включения в ЕРРП, рег. номер	Компания-разработчик
PostgreSQL	Postgres Pro	18.03.2016, № 104	«Постгрес Профессиональный»
PostgreSQL	Jatoba	20.09.2019, № 5749	«Газинформсервис»
Greenplum	Arenadata Analytical DB	07.04.2020, № 6481	«Аренадата Софтвер»
PostgreSQL	Proxima DB	07.10.2020, № 6986	«Орион»
PostgreSQL	Arenadata Postgres (ADPG)	07.06.2022, № 13849	«Аренадата Софтвер»
Greenplum	SDP AnalyticDB	13.02.2023, № 16610	Сбербанк России
PostgreSQL	«Квант-Гибрид»	09.08.2023, № 18509	«Квантом» («Концерн Гранит»)
Greenplum	Data Ocean.Analytical WareHouse	27.11.2023, № 20026	«ДатаБленд»

Источник: ЕРРП

пании. В основном это крупный и средний бизнес, который развивает аналитические системы и строит корпоративное хранилище данных в облаке. Например, на платформе Yandex Cloud компания «М.Видео» создала рекомендательную систему, а Hoff – масштабируемое хранилище данных для продуктовой и маркетинговой аналитики.

Также используют DBaaS в медицине, телекоме, промышленности, логистике и транспортной отрасли. Один из ключевых сценариев – создание единого корпоративного хранилища данных для разных задач: для подготовки отчетности, запуска продуктов и операционной деятельности компании. СУБД служит для поддержания отдельных приложений и сайтов, для аналитики в реальном времени. Кроме того, компании стали чаще обрабатывать данные в облаке для дальнейшего анализа с помощью технологий машинного обучения и искусственного интеллекта.

DBaaS – отличная возможность протестировать разные решения без значительных финансовых вложений, поэтому сервис пользуется спросом у разработчиков. «Основные пользователи DBaaS – компании, которые создают собственные продукты по микросервисной модели, а также те, кто выполняет разработку крупных систем на основе больших баз данных, таких как CRM, ERP и т.д. В первую очередь DBaaS используют для построения cloud native-решений», – указывает В. Шульга.

◀ **Рис. 2. Крупнейшие игроки рынка DBaaS в России в 2023 г. (прогноз), млн руб.**

Источник: iKS-Consulting

Источник: iKS-Consulting

▲ **Рис. 3. Прогноз рынка DBaaS в России 2023–2025 гг., млрд руб.**

Прогнозы и перспективы

Спрос на качественную работу с данными в облаке – хранение, обработку, анализ и визуализацию – постоянно повышается. «Потребление сервисов платформы данных Yandex Cloud выросло вдвое, а число клиентов этой группы сервисов – в 1,2 раза», – констатирует В. Грабельников. Он считает, что построение единой платформы для работы с данными – главный долгосрочный тренд и ее наличие уже обязательно для решения аналитических задач. Это обусловлено, с одной стороны, усложнением задач, с другой – ростом числа аналитиков в командах. «Если команда использует один источник данных, но разные инструменты анализа, то неминуемы разнобой в конвейерах задач и задержки в выполнении бизнес-запросов», – предостерегает эксперт.

Этот же тренд отмечает и директор бизнес-юнита «КРОК Облачные сервисы» Сергей Зинкевич: «Раньше клиента интересовало только само облако: виртуальные машины, процессор, память. Теперь практически каждый клиент облака имеет список нужных DBaaS, так как понимает, что даже если сейчас он не будет их использовать, то в недалеком будущем обязательно к этому придет».

Сегодня в России сервис DBaaS предлагают все крупные облачные провайдеры. На рынке представлена широкая линейка облачных баз данных. По оценкам экспертов «Ростелекома», рынок DBaaS будет расти в среднем на 20–30% в год. Подтолкнуть к переходу на облачные базы данных может как недостаток высококвалифицированных ИТ-специалистов в штате, так и желание сократить нецелевые (не связанные с профильным бизнесом) капитальные затраты. Дальнейшее развитие пойдет по пути повышения качества, гибкости и скорости предоставления сервисов.

Пока среди российских заказчиков сервисы DBaaS не слишком распространены – по данным iKS-Consulting, 63,9% опрошенных ими не пользуются. Но перспективы большие: аналитическое агентство прогнозирует рост рынка DBaaS в РФ примерно на 24–32% ежегодно в ближайшие несколько лет (рис. 3). Этому способствует более широкое применение сложных операций (аналитики) и сопутствующих сервисов, таких как BI и ETL, нужных при миграции данных из одного источника в другой. В числе других факторов роста – прекращение поддержки со стороны западных вендоров СУБД, дефицит кадров и никем не отмененные задачи цифровизации страны.

Данные стали ценным ресурсом, который может стимулировать инновации, улучшать процесс принятия решений и создавать новые возможности для бизнеса. Мир погружается в глобальную цифровую экосистему – экономику данных, и без облачных «библиотекарей» обойтись будет невозможно. ИКС

Облако-суперкомпьютер

Николай Носов

Серийный болид

Согласно опубликованному в ноябре 2023 г. списку Top500 самых мощных нераспределенных компьютерных систем в мире, на третьем месте оказался дебютант – Microsoft Azure Eagle supercomputer, обогнавший лидировавший в 2020–2021 гг. японский суперкомпьютер Fugaku, который откатился на четвертое место. Это самая высокая позиция, которой облачная система когда-либо достигала в Top500.

Гонку суперкомпьютеров можно сравнить с соревнованиями болидов «Формулы-1». Каждый болид – уникальное произведение искусства, плод многолетних изысканий инженеров и технологов, где значение имеет каждый винтик, каждый изгиб корпуса. Невозможно представить, чтобы на таких гонках победила пусть и подготовленная, но серийная машина.

Но в гонке суперкомпьютеров это оказалось возможным, что многие эксперты оценивают как слом парадигмы. Компания Microsoft развернула суперкомпьютер в своем облаке Azure на стандартных модулях, объединив их в единую систему, включающую более миллиона ядер. Результаты выполнения тестов LinPack на этой системе позволили обогнать бывшего лидера из Японии. Вычислительную систему не строили годы, как конкуренты, «тюнинг» сделали за шесть месяцев. И даже интерконнект не кастомизированный, не создавался для конкретной установки, как у остальных игроков из первой четверки, а относительно независимый – на базе Infiniband.

	Frontier	Aurora	Eagle	Fugaku
CPU	**AMD** Optimized 3rd Generatio EPYC	**Intel** Xeon CPU Max 9470 52C 2.4GHz	**Intel** Xeon Platinum 8480C 48C 2GHz	**Fujitsu** Fujitsu ARM A64FX 48C 2.2GHz
Ускоритель	**AMD** AMD Instinct MI250X	**Intel** Intel Data Center GPU Max	**NVIDIA** NVIDIA H100	–
Интерконнект	**HPE** HPE Slingshot-11	**HPE** HPE Slingshot-11	**NVIDIA** NVIDIA Infiniband NDR	**Fujitsu** Tofu interconnect D
Инфраструктура	**HPE**	**HPE**	**Microsoft**	**Fujitsu**

◀ Рис. 1. Основные параметры первой четверки суперкомпьютеров

Источник: Институт программных систем им. А.К. Айламазяна РАН

▲ **Рис. 2. Суперкомпьютер Frontier**

В Eagle используется не экзотическая системная архитектура, ориентированная только на высокопроизводительные вычисления, а облачная платформа Microsoft Azure и стандартная аппаратная платформа, основанная на процессорах Intel Xeon Platinum 8480C и графических ускорителях Nvidia H100, какие применяются для задач искусственного интеллекта (рис. 1). И это будет доступный всем, а не только отдельным компаниям по разрешению, облачный сервис.

Экзафлопсный мир

В 2023 г. всю призовую тройку составили американские суперкомпьютеры. Первую строчку с 2022 г. с производительностью 1,19 экзафлопс (пиковая – 1,69 экзафлопс) удерживает развернутый в Национальной лаборатории Оук-Ридж (ORNL) в Теннесси суперкомпьютер Frontier (рис. 2). Экзафлопсный суперкомпьютер – лучшее изобретение человечества 2023 г., по версии американского журнала Time, – основан на новейшей архитектуре HPE Cray EX235a и оснащен процессорами AMD EPYC 64C с частотой 2 ГГц. Общее количество ядер системы – 8 699 904, показатель энергоэффективности – 52,59 гигафлопс/Вт, а для передачи данных используется сеть (интерконнект) HPE Slingshot-11 (совместная разработка HPE и Cray). Мощность установки – как у крупного ЦОДа, 22,7 МВт.

На втором месте – Aurora, созданная вернувшейся в большую гонку компанией Intel. Суперкомпьютер основан на кластерной системе HPE Cray EX, в которой используются блейд-компьютеры Intel Exascale Compute Blade на базе процессоров Intel Xeon CPU серии Max и ускорителей Intel Data Center GPU серии Max. С этим суперкомпьютером связывает большие надежды Human Brain Project, проект изучения человеческого мозга. Исследователи попытаются расшифровать человеческий коннектом, т.е. получить детальное описание структуры нервных связей и организации нервной системы человека. Потенциал у системы большой – после окончательной настройки ее пиковая производительность составит 2 экзафлопс.

Мир, хотя и с небольшой задержкой, достиг экзафлопсной стадии развития вычислительной техники. На протяжении 44 лет до 2008 г. мощность процессоров удваивалась каждые 18 месяцев, производительность систем увеличивалась на три порядка каждые 11 лет. Из-за технологических трудностей процесс замедлился, и рубеж в 1 экзафлопс вместо 2019 г. был перейден только в 2022 г. А следующий рубеж – 1 зеттафлопс (10^{21}), по оценкам Института программных систем им. А.К. Айламазяна РАН, будет преодолен только в 2035–2037 гг.

В ноябре 2023 г. впервые «перевыполнен» закон Парето – 20% суперкомпьютеров обеспечивают более 80% суммарной мировой производительности по тестам LinPack. Такая картина не

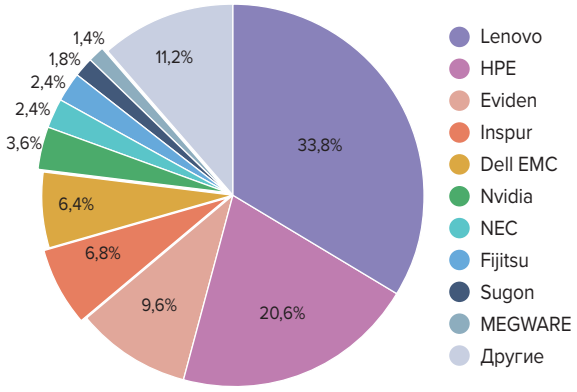
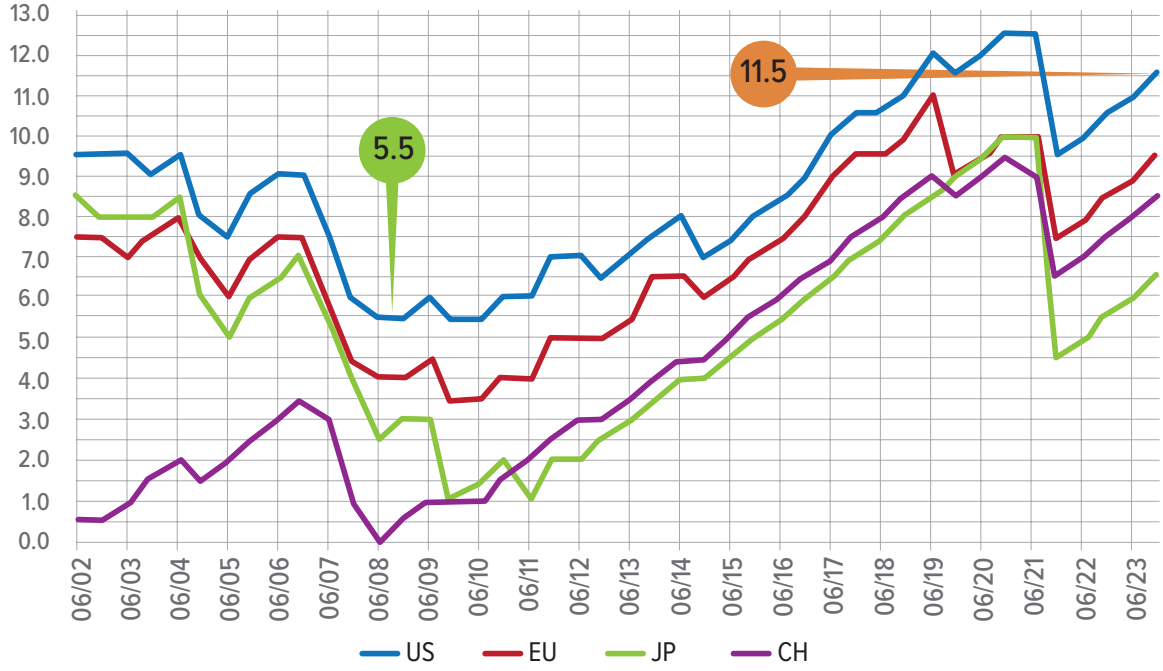


Рис. 3. ▶ Доля вендоров вычислительных систем в числе суперкомпьютеров рейтинга Top500

Источник: www.top500.org



◀ Рис. 4. Отставание России по сумме Rmax от США (US), Евросоюза (EU), Китая (CH) и Японии (JP)

Источник: Институт программных систем им. А.К. Айламазяна РАН

наблюдалась ни в одном из 63 предыдущих выпусков Top500. Причем на четыре лидера приходится 39,6% совокупной производительности суперкомпьютеров списка.

Не так давно возглавлявшие рейтинг китайские суперкомпьютеры из первой десятки выбыли, но зато китайские вендоры резко увеличили число проданных, пусть и более слабых суперкомпьютеров.

На долю компании Lenovo приходится 33,8% суперкомпьютеров, на долю Inspur – 6,8%, Sugon – 1,8% (рис. 3). Реальную картину по высокопроизводительным решениям оценить трудно, поскольку Китай ушел в тень. 11 суперкомпьютерных компаний Китая находятся под санкциями и перестали публиковать данные о новых проектах, поэтому в рейтинге остались только старые топовые установки.

По какому пути идти России?

В России за год ничего не изменилось – в Top500 по-прежнему семь отечественных суперкомпьютеров: «Червоненкис», «Галушкин» и «Ляпунов» компании «Яндекс», Christofari Neo и Christofari от Сбера, «Ломоносов-2» (МГУ) и MTS Grom. При этом российский лидер «Червоненкис» в 55 раз отстает по производительности от самого мощного компьютера мира. Шесть из семи российских суперкомпьютеров принадлежат коммерческим организациям и в основном решают их задачи. Это вызывает озабоченность в научных кругах, представители которых выступают с призывами построить в стране более сбалансированную суперкомпьютерную инфраструктуру с большей долей государственных суперкомпьютеров для научных задач.

В 2008 г. отставание России по совокупной вычислительной мощности суперкомпьютеров из Top500 (Rmax) составляло 5,5 лет, а по уровню развития технологий – всего 2,5 года. В 2022 г. новых суперкомпьютеров в стране не появилось, отставание по Rmax от лидеров увеличилось и достигло 11,5 лет.

Ситуация в суперкомпьютерной отрасли в России непростая и стала еще более сложной из-за санкций и кадровых проблем. О полном импортозамещении можно только мечтать, но экспертиза в основных направлениях еще есть.

Необязательно налаживать параллельный импорт из недружественных стран. Так, в Китае в ответ на американские санкции, запрещающие поставку в страну современных ускорителей, за два года создали сокет-совместимый с Xeon Phe ускоритель Matrix-2000 для собственного суперкомпьютера Tianhe-2. Можно ориентироваться на опыт нашего соседа.

Вместе с тем успех суперкомпьютера Eagle показывает, что отличных результатов могут добиться и коммерческие компании, предлагающие услуги высокопроизводительных вычислений по сервисной модели. Эффективнее не строить суперкомпьютеры с нуля в каждом вузе, а использовать уже имеющийся опыт создания и эксплуатации российских высокопроизводительных систем коммерческими организациями. Особенно это касается разработки моделей для искусственного интеллекта. Государственные субсидии можно выделять непосредственно научным группам для аренды суперкомпьютерных мощностей по сервисной модели, что послужит и развитию отрасли. ИКС

Там, где облако встречается с периферией

Оуэн Роджерс, директор по исследованиям в области облаков, Uptime Institute

Необходимость уменьшить временну́ю задержку при работе приложений заставляет облачных провайдеров находить различные варианты приближения облачной инфраструктуры к конечным пользователям. Но стоимость и отказоустойчивость этих решений также различны.

Снижение задержки – основная причина, по которой облачные провайдеры предлагают периферийные (edge-) узлы как часть своей облачной инфраструктуры. Всего несколько лет назад те же провайдеры утверждали, что публичное облако, размещенное в гиперЦОДе, подходит для большинства задач. Но поскольку клиенты настаивали на уменьшении задержки и улучшении контроля над данными, они смягчили свою позицию и разработали варианты, которые позволяют развертывать ПО публичного облака ближе к заказчикам, тем самым уменьшая задержку при предоставлении облачных сервисов (см. рисунок).

Эти шаги обусловлены тем, что для эффективной работы целого ряда приложений – игр, потокового видео и управления процессами в режиме реального времени – требуется малая задержка. Конечным пользователям, и частным, и корпоративным, нужны более продвинутые функции с меньшим временем отклика, и поставщики облачных приложений такие функции готовы предоставить. Они и сами заинтересованы в том, чтобы уменьшить затраты на перемещение данных по сети на большие расстояния и снять возникающие при этом ограничения на пропускную способность. В результате спрос на хранение и обработку данных вблизи мест их использования возрастает еще больше.

Облачные провайдеры обычно рассматривают периферийную инфраструктуру – и на границе с площадкой заказчика, и на самой площадке (on-premises) – как расширение публичного облака (в конфигурации гибридного облака), а не как изолированные частные облака, работающие независимо. Они считают свои гиперЦОДы основным местом размещения рабочих нагрузок, а периферийные узлы предлагают использовать для специальных задач, для которых централизованное облако не подходит. По сути, провайдеры рассматривают периферийные узлы как тактические промежуточные пункты.

Облачные провайдеры не хотят, чтобы клиенты считали периферийные узлы столь же многофункциональными, как основную облачную инфраструктуру в гиперЦОДах. Поэтому на периферии они предлагают лишь ограниченное количество сервисов для специальных задач. Поскольку периферийная инфраструктура использует основное облако для некоторых аспектов администрирования, существует риск утечки данных и потери контроля над edge-узлами. Кроме того, соединение между основным облаком и edge-облаком потенциально является единой точкой отказа.

Инфраструктура как сервис

Поставщики услуг IaaS обычно используют термин «регион» для описания географической области, в которую входят несколько независимых зон доступности (availability zone, AZ). Каждая зона доступности состоит из минимум

одного ЦОДа. В стране может быть много регионов, в каждом из которых, как правило, две или три AZ.

Облачные провайдеры также предлагают городские (metro) сайты и локации рядом с площадками заказчиков (near-premises). Эти узлы представляют собой специализированные программно-аппаратные комплексы (edge-ПАК), расположенные в небольших ЦОДах или в дата-центрах, которые предоставляют услуги colocation. Провайдеры управляют этими периферийными узлами так же, как и зонами AZ. Задержка между такими узлами и конечными пользователями составляет несколько миллисекунд. Однако периферийные облачные узлы обычно обладают меньшими функциональными возможностями и меньшей отказоустойчивостью при более высокой цене по сравнению с зонами AZ в более крупных ЦОДах.

Кроме того, такая периферийная инфраструктура не может охватывать всю территорию страны – она создается только там, где спрос на услуги оправдает инвестиции, как правило, в городах. Скорость передачи данных между периферийными узлами облачных провайдеров и конечными пользователями зависит от характеристик имеющейся сетевой инфраструктуры и доступности сетей 4G или 5G.

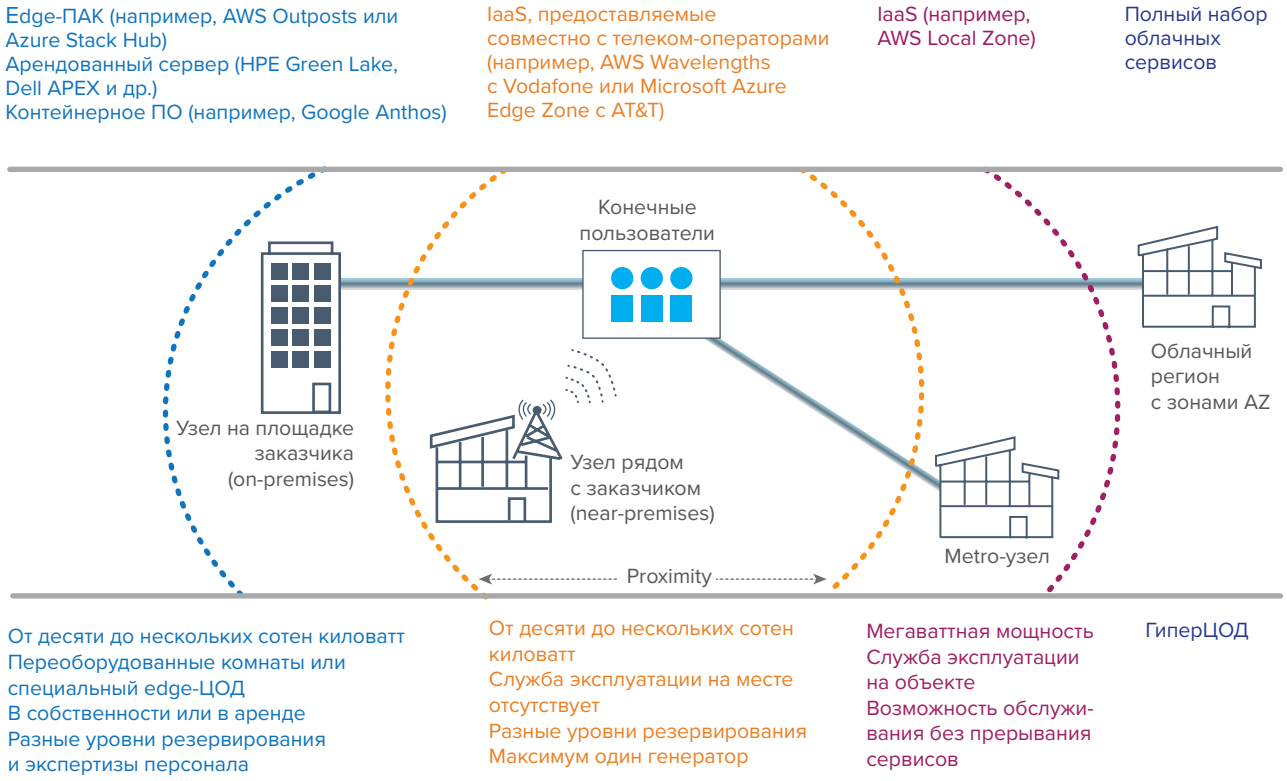
Когда клиент хочет развернуть приложение в облаке, он сначала выбирает регион и зону AZ, используя графический пользовательский интерфейс или API облачного провайдера. Периферийные узлы предлагаются ему в качестве вариантов развертывания наравне с основным регионом. Если подходящая периферийная локация имеется, то получить IaaS-ресурсы в ней обычно можно за считанные минуты.

Metro-узлы

Узлы уровня metro не предоставляют такого набора облачных сервисов, как регионы. В них предлагаются в основном вычислительные ресурсы, хранение данных, управление контейнерами и балансировка нагрузки. В регионе есть несколько зон AZ, а на metro-уровне зона, как правило, одна, поэтому на ее основе нельзя создать полностью отказоустойчивое приложение. Таким образом, пользователи должны понимать, что, хотя облачные edge-сервисы могут уменьшить время задержки и затраты на каналы связи, отказоустойчивость может быть ниже. Metro-узлы обычно ориентированы на графически насыщенные приложения, такие как виртуальные рабочие столы, видеоигры, обработка видео, аудио или сенсорных данных в режиме реального времени.

Вместе с тем сервисы на уровне metro могут соответствовать требованиям к отказоустойчивости большинства корпоративных приложений. ЦОДы, поддерживающие работу metro-уз-

Различные варианты размещения периферийных (edge-) узлов облачной инфраструктуры в рамках модели гибридного облака ▼



Источник: Uptime Intelligence, 2023

лов, обычно имеют мегаваттную мощность, укомплектованы службой эксплуатации и построены таким образом, чтобы можно было осуществлять обслуживание без перерыва в предоставлении сервисов, а конечные пользователи подключаются по резервированным оптоволоконным каналам.

Узлы рядом с заказчиками (near-premises)

Как и metro-локации, узлы, расположенные вблизи заказчиков, предоставляют менее широкий спектр услуг, чем зоны AZ и регионы. Существенное отличие от metro-локаций в том, что такие узлы развертываются непосредственно в инфраструктуре сетей 4G или 5G, возможно, на ближайшем сайте сотовой сети. Это сокращает число сетевых пролетов (hop), а значит, и время задержки в условиях перегрузки.

Для развертывания узлов near-premises облачные провайдеры обычно сотрудничают с крупными телеком-операторами, например, в США сервис AWS Wavelengths предоставляется в партнерстве с Vodafone, а сервис Microsoft Azure Edge Zone – с участием AT&T. Варианты использования этих решений могут включать работу приложений реального времени, таких как обработка и анализ видео в реальном времени, поддержку автономных транспортных средств и систем дополненной реальности. 5G обеспечивает подключение там, где отсутствует инфраструктура фиксированной связи, или в местах временного развертывания.

Местами размещения узлов near-premises могут быть сайты сотовой сети или узлы связи, типовая мощность – от десятков до нескольких сотен киловатт. Обслуживающий персонал на этих узлах обычно отсутствует (контроль осуществляется дистанционно), уровень резервирования может быть разным (с одним генератором или без такового).

Узлы у заказчика (on-premises)

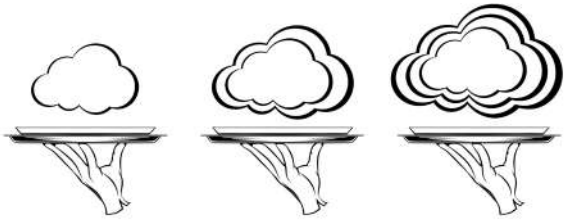
Облачные провайдеры также предлагают аппаратное и программное обеспечение, которое может быть установлено в том ЦОДе, который выберет заказчик. Последний несет ответственность за все аспекты управления ЦОДом и его техническое обслуживание, в то время как облачный провайдер управляет оборудованием или ПО удаленно. Плата за услуги провайдера обычно взимается соразмерно объему потребляемых ресурсов в течение согласованного срока. Клиент может предпочесть этот вариант, если рядом нет подходящих облачных периферийных узлов или если регуляторные или корпоративные правила требуют от него использования собственных центров обработки данных.

Поскольку заказчик сам выбирает место для размещения облачной инфраструктуры, характеристики соответствующего ЦОДа и его оснащение могут быть разными. Типовая мощность объекта – от десяти до нескольких сотен киловатт; он может быть в собственности или аренде; размещаться в переоборудованных помещениях или использовать специальные решения для организации edge-ЦОДов. Уровни избыточности и квалификации персонала также разнятся от одного проекта к другому. Некоторые поставщики оборудования для периферийных дата-центров предоставляют дополнительные услуги удаленного мониторинга. Подключение может осуществляться через линии связи или локальное оптоволокно, задержка сигнала между площадкой и конечным пользователем также значительно варьируется.

Поставщики услуг colocation все чаще стараются выделиться на рынке за счет прямого пиринга с сетями облачных провайдеров, чтобы сократить время задержки сигнала. Например, Google Cloud рекомендует свой сервис Interconnect для задач, в которых задержка между публичным облаком и узлом colocation не должна превышать 5 мс. К Google Cloud подключены уже более 140 сайтов colocation, в том числе принадлежащие компаниям Equinix, NTT, Global Switch, Interxion, Digital Realty и CenturyLink. Другие облачные провайдеры имеют схожие договоренности с поставщиками услуг colocation.

Три варианта решений on-premises

Существуют три основных варианта расширений облака, которые могут быть размещены у заказчика. Они различаются главным образом тем, насколько легко настроить комбинацию аппаратного и программного обеспечения. Специализированное edge-устройство (edge-ПАК) просто в инсталляции, но имеет ограниченные возможности настройки; сервер с оплатой по мере использования (pay-as-you-go) обеспечивает гибкость в выборе производительности и интеграции с облаком, но требует дополнительной настройки; наконец, контейнерная платформа обеспечивает гибкость в выборе аппаратного и программного обеспечения и возможности мультиоблачной работы, но требует высокого уровня экспертизы персонала.



Edge-ПАК. Это предварительно сконфигурированное устройство с предустановленным ПО оркестрации. Клиент размещает его в своем ЦОДе для подключения к провайдеру публичного облака. У него есть ограниченная возможность конфигурирования такого устройства, но, как правило, нет прямого доступа к аппаратному обеспечению и ПО.

Разворачивание ИТ-ресурсов осуществляется с помощью того же графического интерфейса и API-интерфейсов, которые используются при работе с основным облаком в регионах и зонах AZ. В большинстве случаев для задач администрирования требуется подключение к публичному облаку. Устройство остается собственностью поставщика облачных услуг, и покупатель обычно арендует его, скажем, на три года. Примеры: AWS Outposts, Azure Stack Hub и Oracle Roving Edge Infrastructure.

Сервер pay-as-you-go. Это физический сервер, сдаваемый в аренду клиенту и оплачиваемый им соответственно выделенным и потребленным ресурсам. Провайдер обслуживает и обновляет сервер, удаленно учитывает потребление ресурсов, предлагая при необходимости увеличить производительность. Он может также установить на сервер ПО – с оплатой по тому же принципу. Такое ПО может состоять из инструментов облачной оркестровки, которые предоставляют возможности частного облака и подключения к публичному облаку для реализации гибридной модели. Клиенты могут выбирать технические характеристики оборудования и использовать ПО не только облачного провайдера, но и третьей стороны. Примеры: HPE Green Lake и Dell APEX.

Контейнерное ПО. Клиенты также могут выбрать собственное сочетание аппаратного и программного обеспечения с контейнерами в качестве базовой технологии для взаимодействия с публичным облаком. Контейнеры позволяют разбивать программные приложения на множество небольших функций, которые можно поддерживать и масштабировать по отдельности и которыми можно так же управлять. Их переносимость позволяет приложениям работать, будучи распределенными по разным местам.

Облачные провайдеры предлагают управляющее ПО для удаленных узлов, совместимое с публичными облаками. Примерами могут служить Google Anthos, IBM Cloud Satellite и Red Hat OpenShift Container Platform. В этом варианте клиенты могут выбирать свое аппаратное обеспечение и некоторые компоненты ПО для оркестрации (например, контейнерные движки), и они также сами отвечают за построение системы и управление сложным набором компонентов.

Итоги

Заказчики могут быстро и легко размещать приложения в периферийных узлах, предлагаемых облачными провайдерами на metro-уровне или в близлежащих локациях. Там, где подходящий узел недоступен или заказчик предпочитает использовать локальные ЦОДы (на своей территории), у него есть несколько вариантов расширения возможностей публичного облака до edge-ЦОДа.

Периферийные узлы различаются по уровню отказоустойчивости, доступности и – самое главное – по времени задержки сигнала. Как уже говорилось, именно снижение задержки – основная мотивация для развертывания облака на периферии. Как правило, заказчики платят больше за развертывание приложений в периферийных узлах, чем в облачном регионе. Если нет необходимости в малой задержке, периферийные локации могут оказаться неоправданно дорогими.

При развертывании приложений в гибридных средах заказчики должны учитывать вопросы устойчивости их работы. Периферийные узлы обладают меньшей отказоустойчивостью, могут быть не укомплектованы обслуживающим персоналом и характеризуются более высокой вероятностью выхода из строя (по сравнению с центральными узлами облачной инфраструктуры). Приложения должны быть спроектированы таким образом, чтобы могли продолжить работу в случае сбоя в периферийном узле.

Если нет необходимости в малой задержке, периферийные локации могут оказаться неоправданно дорогими

Периферийные узлы и продукты облачных провайдеров, как правило, не предназначены для самостоятельной (изолированной) работы – они ориентированы на использование в качестве расширений публичного облака для определенных задач. Часто управление локальными и периферийными узлами осуществляется с помощью тех же интерфейсов, которые применяются для работы с основным облаком. Если соединение между периферийным узлом и основным облаком прервется, этот узел может продолжить работу, но развертывание новых ресурсов будет невозможно до тех пор, пока связь с публичным облаком не восстановится.

Одной из причин использования периферийных узлов заказчики часто называют необходимость усиления защиты данных. Однако поскольку такие узлы должны быть постоянно подключены к публичному облаку, существует риск непреднамеренной утечки пользовательских данных или метаданных в это облако, что приведет к нарушению требований безопасности. Это надо понимать, и соответствующим риском надо управлять. ИКС

Информационная безопасность: турбулентный 2023

Николай Носов

Атак на информационную инфраструктуру страны и на граждан стало больше, их профиль изменился. Меры защиты, которые принимаются государством и бизнесом, дают свои плоды, но болевых точек по-прежнему много.

События февраля 2022-го резко обострили ситуацию в сфере информационной безопасности. Не улучшилась она и в 2023 г. Одни эксперты считают, что кибервойна России уже объявлена, другие – что настоящая война, с использованием штатных кибервойск, а не прокси из хакерских группировок, еще впереди. Но все согласны, что атак стало больше, проблемы кибербезопасности вышли на первый план и ими невозможно не заниматься.

«Мы фиксируем около 170 целевых атак на российские ресурсы в день. За 2023 г. в сеть утекло более 445 млн строк конфиденциальных данных», – признал на SOC-Forum 2023 старший вице-президент «Ростелекома» по информационной безопасности, генеральный директор ГК «Солар» Игорь Ляпунов. Число событий информационной безопасности (ИБ) в III квартале 2023 г. по сравнению с аналогичным периодом 2022 г. выросло на 85%, число критичных инцидентов – в полтора раза. Средний ущерб от атак хакеров для одной компании за год составил 20 млн руб.

Изменился и профиль атак (рис. 1). «В этом году ландшафт угроз и характер атак поменялись, и прежде всего с точки зрения целей, преследуемых злоумышленниками. Самое заметное изменение – уменьшение числа атак для “раскручивания” инфоповодов», – констатировал заместитель директора Национального координационного центра по компьютерным инцидентам Петр Белов.

С 60 до 15% снизилась доля фейковых сообщений об утечках, но количество самих утечек выросло. Несмотря на то что за год в пять раз уменьшилось число DDoS-атак (60% из них приходится на госресурсы), общее число атак, направленных на нарушение функционирования систем, увеличилось вдвое. Если в 2022 г. было много простых беспорядочных атак на все российские ресурсы, то в 2023-м стало больше целевых атак на КИИ, причем с целью разрушения информационной системы, а не получения выкупа.

Защита КИИ

События последних двух лет показали своевременность принятия в 2017 г. закона «О безопасности критической информационной инфраструктуры РФ». Без реализованных под давлением регуляторов мер негативные последствия действий хакеров были бы значительно серьезнее. Работы далеки от завершения, но уже то, что руководители компаний обратили внимание на обеспечение информационной безопасности и стали вкладывать в нее ресурсы, безусловно положительно сказалось на защищенности страны в киберпространстве.

В 2023 г. работы ускорились. Как сообщил заместитель директора ФСТЭК России Виталий Лютиков, ведомство рассмотрело в три раза больше сведений об объектах КИИ, чем в 2022 г. При этом в целом ряде случаев было выявлено, что на первом этапе – категорировании объектов – их владельцы пытались уменьшить оценочную сумму потенциального ущерба от атак, понизить категорию объекта КИИ и таким образом сэкономить на его защите.

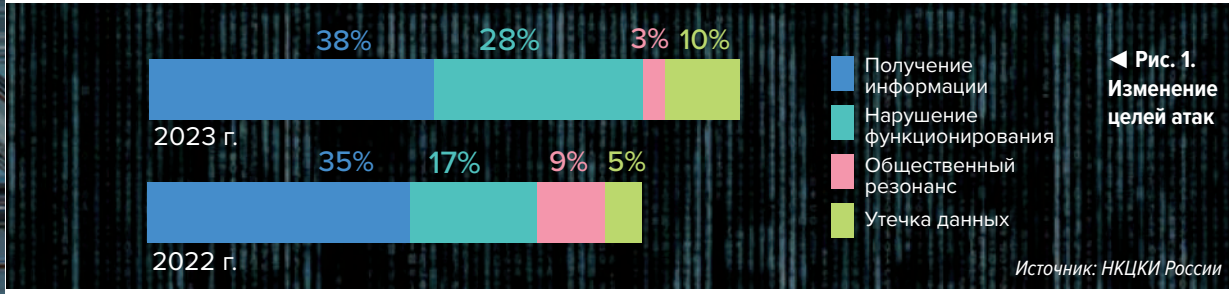
ФСТЭК борется с таким подходом. За последний год с участием привлеченных специалистов было проверено более 40 тыс. систем, и треть систем отправлена на пересмотр категорийности. Типовые недостатки:

- исключение из категорирования объектов, обеспечивающих основные производственные процессы;
- преуменьшение возможных негативных последствий;
- исключение из рассмотрения информационных угроз как причины нарушения штатного функционирования;
- необоснованное разделение объектов с целью занижения категории значимости.

В помощь компаниям отраслевые регуляторы разработали согласованные с ФСТЭК перечни типовых объектов, подлежащих категорированию, и методические рекомендации по отнесению систем к различным категориям значимости.

ФСТЭК наладила государственный контроль объектов КИИ, в результате которого было выявлено более 700 нарушений. Наиболее частые нарушения (в том числе на значимых объектах КИИ) таковы:

- не реализовано обновление антивирусных баз;
- не настроены средства антивирусной защиты;



◀ Рис. 1. Изменение целей атак

Источник: НКЦКИ России

- администрирование осуществляется с рабочих мест корпоративной сети с выходом в интернет, для которых не реализованы меры обеспечения безопасности;
- используется уязвимое ПО без принятия компенсирующих мер обеспечения безопасности;
- не проведены мероприятия по выявлению, анализу и устранению уязвимостей на значимых объектах КИИ.

«Каждая вторая система, проверенная нашей службой, имеет критические уязвимости. В 2023 г. по сравнению с предыдущим их число увеличилось в 2,5 раза», – отметил В. Лютиков. Одна из главных причин – прекращение поддержки зарубежными вендорами своих информационных систем, установленных на российских объектах. Кроме того, в условиях ускоренного импортозамещения разработчики отечественного ПО уделяют недостаточно внимания информационной безопасности создаваемых продуктов и используемых open source-компонентов.

ЦОД как угроза

Серьезная проблема, которую пока не удалось решить, – формулирование и предъявление подрядчикам требований по информационной безопасности. Большая часть публичных инцидентов была так или иначе связана с входом в инфраструктуру жертвы через подрядные организации. По данным Positive Technologies, число атак supply chain («атака через цепочку поставок») и trusted relationship («атака через доверительные отношения») за три квартала 2023 г. по сравнению с аналогичным периодом 2022 г. выросло вдвое.

Большая часть публичных инцидентов была так или иначе связана с входом в инфраструктуру жертвы через подрядные организации

Государство в первую очередь беспокоит защита государственных систем. «К сожалению, ни на уровне законодательства, ни на уровне договоров не установлены требования к подрядным организациям по обеспечению безопасности. Это касается и телекоммуникационной инфраструктуры, особенно предназначенной для размещения и функционирования на ней государственных систем. Большинство ЦОДов не отнесено к государственным. Формально на них требования не распространяются, и госорганизациям сложно даже обосновать необходимость траты денег на обеспечение в них информационной безопасности. Мы эту проблему понимаем. Сделан первый шаг – разработан законопроект об установлении требований по защите госресурсов вне зависимости от места обработки информации», – рассказал В. Лютиков.

Облачные провайдеры и операторы ЦОДов не могут и не должны разбираться в бизнес-процессах клиентов и, следовательно, отвечать за их защиту. Но могут предоставлять услуги в соответствии с требованиями, предъявляемыми к информационной безопасности. Уже стал стандартным сервис развертывания системы в защищенном контуре, обеспечивающем защиту персональных данных согласно законодательству. В случае принятия упомянутого законопроекта появится новая услуга – размещение информационной системы в защищенном контуре, удовлетворяющем требованиям по защите государственных информационных систем. А у заказчиков – обоснование расходования бюджетных средств на такую услугу.

Хакеры против хакеров

Выполнение требований регуляторов снижает риски, но не дает гарантий безопасности. Если компания хочет убедиться в надежности защиты информационных систем, стоит предложить ее взломать профессионалам.

Наиболее уверенные объявляют программу bug bounty – предлагают атаковать себя всем желающим, а добившимся в поиске уязвимостей успеха выплачивают вознаграждение. Пионером в использовании такого подхода в России стала компания «Яндекс»; выплачивает вознаграждения за обнаруженные уязвимости и VK. На SOC-Forum 2023 программу bug bounty анонсировала компания Innostage.

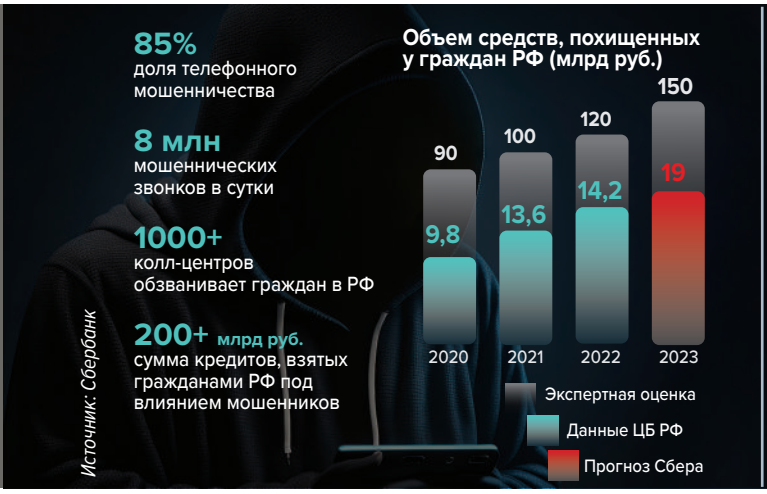
Однако часто компании не готовы подставить действующую инфраструктуру под атаку даже «белых» («этичных») хакеров. Ведь атака может привести к необходимости восстановления ИТ-инфраструктуры и остановке бизнес-процессов. Безопаснее смоделировать инфраструктуру на киберполигоне, предложить ее атаковать проверенным хакерам (команде «красных»), а свои ИБ-службы тренировать в защите и разборе инцидентов в команде «синих».

В России услуги киберполигона предлагают компании BI.ZONE (Cyber Polygon), Positive Technologies (The Standoff), «Инфосистемы Джет» (Jet CyberCamp) и «Ростелеком» (Национальный киберполигон и платформа «Солар Кибермир»).

Атаки на граждан

По оценкам Сбербанка, в 2023 г. 85% похищенных у россиян средств были украдены с помощью телефонного мошенничества. Граждан России обзванивают более тысячи колл-центров преступников, совершающих 8 млн звонков в сутки (рис. 2). «Принятые меры по борьбе с телефонными мошенниками, в том числе поправки в законы, дали результат, но кардинально ситуацию не изменили», – признал заместитель председателя правления Сбербанка России Станислав Кузнецов.

К сожалению, многие не сообщают об инцидентах мошенничества, не надеясь вернуть украденные средства. В результате, если в 2022 г. ЦБ РФ сообщал о 14,2 млрд руб., похищенных у граж-



▲ **Рис. 2. Хищения у граждан России, совершенные с помощью телефонного и онлайн-мошенничества**

▲ **Рис. 3. Улучшение ситуации в сфере кибербезопасности в 2023 г.**

дан, то по оценкам экспертов эта сумма была почти на порядок больше.

Атаки на граждан идут и в информационном поле. В сутки в мире, по приведенным С. Кузнецовым данным, фиксируется более тысячи фейковых новостей. «Сила информационных атак колоссальная. Мы многое недооцениваем в этой связи», – отметил представитель Сбербанка. Среди новинок – использование искусственного интеллекта для создания фейковых новостей.

Принимаемые против телефонных мошенников меры частично сместили фокус атак на мессенджеры и соцсети. «С 2022 г. мы наблюдаем увеличение количества инцидентов, в которых злоумышленниками были выгружены пользовательские данные с целью получения доступа к аккаунтам мессенджера Telegram Desktop», – сообщил руководитель отдела реагирования на угрозы ИБ экспертного центра безопасности Positive Technologies Денис Гойденко. Причем если в 2022 г. по отношению к предыдущему году число таких инцидентов выросло на 6%, то в 2023 г. – уже на 63%.

Стали сильнее

В 2023 г. продолжилось совершенствование регуляторных мер. Согласно принятым в конце декабря 2022 г. поправкам в Постановление Правительства РФ от 08.02.2018 № 127, начал действовать измененный порядок категорирования объектов КИИ:

- сведения об объектах КИИ подлежат строгому мониторингу на предмет полноты и актуальности;
- с 21.03.2023 отраслевые ведомства вправе формировать перечень типовых отраслевых объектов КИИ, которые обязательно должны входить в перечень объектов КИИ, подлежащих категорированию;
- расширен перечень критериев значимости и изменены значения их показателей.

Новые поправки к закону «О национальной платежной системе» вводят дополнительные требования к системам дистанционных платежей, включая обязательную идентификацию пользователей и защиту персональных данных. Для противодействия переводам денежных средств без согласия клиента в марте 2023 г. Банк России выпустил новые рекомендации СТО БР БФБО (Стандарт Банка России. Безопасность финансовых (банковских) операций) по контролю «цифровых отпечатков устройств» – совокупности параметров устройств пользователя, с которых он обращается для получения услуги.

«Хорошая новость – за год мы стали сильнее. Улучшилось регулирование, быстрее начали реагировать правоохранительные органы», – отметил С. Кузнецов. Согласно данным Сбербанка, рынок кибербезопасности вырос более чем на 20%, аналогичный рост показал рынок киберучений (рис. 3).

Проблемы, конечно, остаются. Так, среди регуляторов нет главного координатора; нет обмена данными о кибератаках в режиме онлайн и единых правил для защиты физических и юридических лиц. Растет дефицит кадров. Кроме того, ненормально, когда российский, значительно менее качественный продукт на порядок дороже, чем западный аналог. Когда, используя монопольное положение на рынке, компания не ориентируется на себестоимость, а назначает произвольную цену. Для противодействия такому подходу С. Кузнецов предложил ввести госприемку по качеству и стоимости отечественных продуктов.

Вместе с тем, как указал И. Ляпунов, оптимизм должен быть профессиональным качеством любого менеджера. «Все беды в головах», – добавил он. Просто проблемы нужно выявлять и работать над их решением. ИКС

В сутки в мире фиксируется более тысячи фейковых новостей

Регулирование ИБ: защищать и развивать

Сложная геополитическая обстановка, санкционное давление и постоянно растущий уровень угроз стимулируют пересмотр мер поддержки и регулирования российских ИБ- и ИТ-отраслей, что отражается в принятых в последние годы на государственном и отраслевом уровне документах.

Николай Носов

Некое обобщение этой деятельности сделал экспертно-аналитический центр ГК InfoWatch, изучив более 1200 выпущенных за последние три года регулирующих документов по ИБ и ИТ и представив результаты своей работы в отчете «Нормативные правовые акты в сфере информационной безопасности и цифровой экономики. Итоги 2021–2023 гг.».

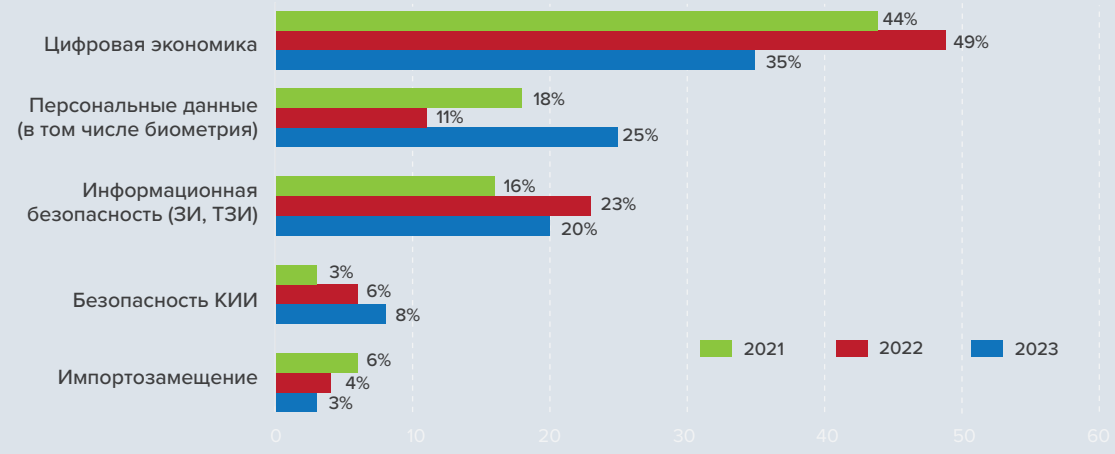
Закономерно, что почти половина принятых документов относится к теме «Цифровая экономика». На второе место (25%) в 2023 г. вышло направление персональных данных (включая биометрические), что можно связать с присвоением Единой биометрической системе государственного статуса и принятием 29.12.2022 закона № 572-ФЗ о биометрических персональных данных. На третьем месте – направление информационной безопасности (защиты информации, технической защиты информации): на его долю в 2023 г. пришлось 20% всех принятых в рассматриваемой сфере документов.

Угрозы объектам критической информационной инфраструктуры за последние три года из теоретической плоскости перешли в практическую, и на это обратили внимание законодатели. Доля принятых документов, относящихся к безопасности КИИ, увеличилась почти в три раза – с 3 до 8%.

К теме импортозамещения интерес регуляторов снизился (3% в 2023 г.). В числе других направлений, не преодолевших пятипроцентный барьер, – «Лицензирование деятельности по технической защите информации», «Национальная безопасность», «Государственная тайна», «Сертификация СЗИ и СКЗИ», «Аккредитация и экспертиза в сфере ИБ и ИТ». Это, вероятно, обусловлено их хорошей проработкой в предшествующий период.

Продолжилась детализация критериев, используемых при классификации отраслевых объектов. Минэнерго России опубликовало перечень типовых отраслевых объектов критической информационной инфраструктуры, функционирующих в сфере энергетики, а Минтранс – в сфере транспорта. Стало ясно, что к объектам КИИ относятся не только, скажем, автоматизированные системы управления аэропортом, но и систе-

Сравнение количества принятых документов по направлениям за 2021–2023 гг. ▶



Источник: InfoWatch

мы контроля оплаты проезда без участия кондуктора.

В декабре 2023 г. на новый этап перешло обсуждение ужесточения наказаний за утечки персональных данных. В Государственную Думу внесены проекты федеральных законов об изменениях в КоАП РФ и УК РФ (в январе 2024 г. они были приняты в первом чтении). Согласно предложенным изменениям, административная ответственность при повторном нарушении устанавливается в виде оборотного штрафа в размере от 0,1 до 3% совокупной выручки за календарный год, предшествующий году, в котором было выявлено нарушение. А УК РФ дополняется статьей 272.1 «Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконного хранения и (или) распространения».

Информационные системы – объекты КИИ их владельцы могут размещать в коммерческих дата-центрах. Поэтому руководитель экспертно-аналитического центра ГК InfoWatch Михаил Смирнов рекомендует операторам коммерческих ЦОДов обратить внимание на новый комплекс документов по безопасности таких объектов. «Заказчики сами или после проверок регуляторов станут выдвигать новые требования, и ЦОДам надо быть к ним готовыми. Кроме того, ЦОДам, которые предоставляют услуги госзаказчикам и предприятиям из стратегических отраслей, стоит обратить внимание на новые документы по импортозамещению. Выполнение новых требований сохранит клиентов и станет конкурентным преимуществом для привлечения новых», – подчеркнул он.

Также эксперт напомнил, что, согласно Постановлению Правительства РФ от 14.11.2023 № 1912, субъекты критической информационной инфраструктуры должны до 1 января 2030 г. перейти на преимущественное применение доверенных программно-аппаратных комплексов для хранения криптографических ключей и сертификатов безопасности, поддержки функций шифрования и аутентификации и защиты системы от атак. Изменения стоит учесть прежде всего владельцам облачных дата-центров, часто предлагающим исключительно программные средства защиты. А ужесточение ответственности за утечки персональных данных, скорее всего, повлияет на востребованность услуг хранения данных в облаке в соответствии с законом № 152-ФЗ, которые предлагают большинство облачных провайдеров.

Кроме того, среди клиентов могут появиться новые субъекты КИИ. Согласно закону от 10.07.2023 № 312-ФЗ, к субъектам КИИ теперь будут относиться и владельцы ИС/ИТС/АСУ из сферы государственной регистрации прав на недвижимое имущество и сделок с ним.

Инстанций, вносящих свой вклад в регулирование отраслей ИТ и ИБ, в нашей стране много. Только по направлению информационной безопасности и цифровой экономики их около десятка: Госдума, Минцифры, ФСТЭК, Роскомнадзор, ФСБ, Минобороны, Минпромторг, Минздрав, Банк России и сам президент. Все регуляторы стараются оперативно реагировать на изменения ландшафта угроз, выпуская соответствующие нормативные акты. И задача бизнеса – их отслеживать и своевременно выполнять содержащиеся в них требования, поскольку на этом основывается успешная работа с клиентами. ИКС

Источники бесперебойного питания для ИТ, промышленности и медицины

Компания ITK представила линейки ИБП Electra Online Box (EOB) и Electra Online Modular (EOM), которые могут использоваться как в ЦОДах и небольших серверных, так и на других предприятиях, где предъявляются повышенные требования к надежности и качеству электропитания оборудования.

EOB – это линейка моноблочных ИБП мощностью 10–600 кВА, в которую входят модели как с трансформатором, так и без него. Возможность подключения в параллель до 4–8 устройств повышает надежность и отказоустойчивость системы. Широкий диапазон входных частот (40–72 Гц) и напряжений обеспечивает надежное электроснабжение подключенных устройств в сетях с нестабильным качеством. ИБП оснащены системой интеллектуального заряда батареи. Коммуникационные порты: RS232, опционально – SNMP.

EOM – это линейка ИБП мощностью 25–500 кВА. Поддерживается возможность параллельной работы до трех устройств для наращивания мощности или резервирования. Максимальная суммарная мощность – 1500 кВА. КПД системы 96,5% в режиме инвертора, в экорежиме – 99%; коэффициент мощности равен 1. Диапазон напряжений 208–480 В. Модульная конструкция обеспечивает «горячую» замену силовых модулей.

Устройства оснащены сенсорным ЖК-дисплеем с диагональю 7 дюймов (модели 125–200) или 10 дюймов (модели 300–500). Совместимы как со свинцово-кислотными, так и с литиевыми батареями (опция).

ИБП EOM отличаются усовершенствованным модулем цифрового управления, интеллектуальным трехэтапным процессом зарядки АКБ с интервалом, интеллектуальным режимом сна, «умной» системой самодиагностики и емким журналом событий, а также технологией цифрового управления циркуляцией воздуха.

www.itk-group.ru

Блок-контейнеры для высокотехнологичного оборудования

Группа компаний ТСС разработала и выпустила специальные блок-контейнеры для систем накопления электрической энергии и другого высокотехнологичного оборудования, которые представляют собой комплектные транспортабельные утепленные модули круглогодичной эксплуатации в габаритах стандартных 20- и 30-футовых контейнеров.

Климатическое исполнение контейнеров, в том числе применяемые при их производстве материалы (сталь, краска и пр.), соответствует нормам использования в умеренном и холодном климате на открытом воздухе (УХЛ1). Степень защиты размещенного в контейнере оборудования от внешних воздействий не менее IP54 (ГОСТ 14254-2015).

Блок-контейнеры оснащаются автоматизированной системой климат-контроля с функцией фрикулинга, поддерживающей температуру внутри в диапазоне от +20 до +25°С при температуре снаружи от –40° до +40°С.

Конструкция контейнеров, а именно наличие трехуровневых фальшполов со съемными секциями дает возможность осмотра и ревизии кабельных линий и воздуховодов. Для удобного доступа к размещенному внутри оборудованию все коммуникации, силовые и вторичные кабельные линии прокладываются в стенах, фальшполах, потолке без применения наружных пластиковых кабель-каналов.

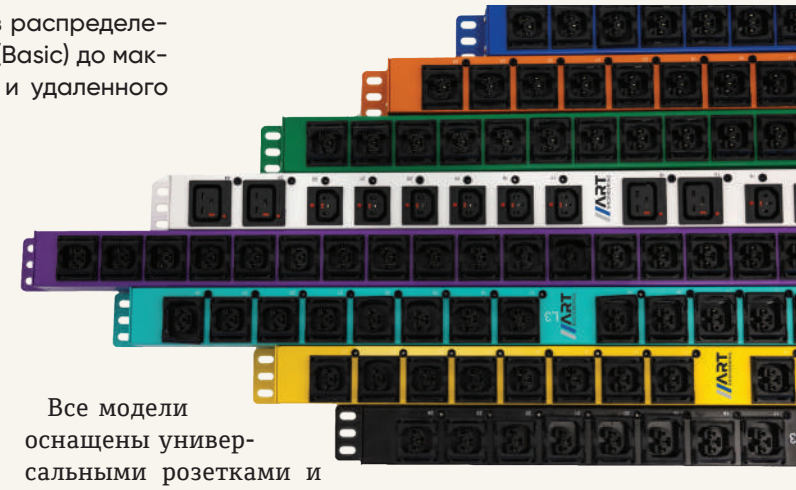
Силовой металлический каркас контейнера имеет достаточную жесткость для загрузки и выгрузки оборудования, а также для транспортирования с оборудованием.

Предусмотрена защита персонала от поражения электрическим током (ГЗЩ и система уравнивания потенциалов). На крыше контейнера имеются закладные пластины под установку изоляторов системы молниезащиты. Также проработана система пожаротушения и охранной сигнализации с дистанционным управлением. Срок службы контейнеров превышает 10 лет.

www.tss.ru

Блоки распределения питания

Компания ART Engineering представляет линейку блоков распределения питания (PDU) различной комплектации: от базовой (Basic) до максимально расширенной с возможностью мониторинга и удаленного управления каждой розеткой.



PDU комплектации Standard, Classic и Function обеспечивают измерение силы тока, частоты, напряжения, активной и полной мощности, а также коэффициента мощности. Точность измерений ± 1%. Поддерживают широкий перечень протоколов: TCP/IP, UDP, DHCP, HTTP, HTTPS, FTP, SNMP v1/2/3, SMTP, Modbus, IPv4, IPv6, Client/Server, Telnet. Устройства оснащены встроенным интеллектуальным контроллером с OLED-дисплеем и допускают возможность каскадирования: объединение в цепь до пяти блоков через порты RS485. Также имеют порты Ethernet, USB и порт для датчиков T/H.

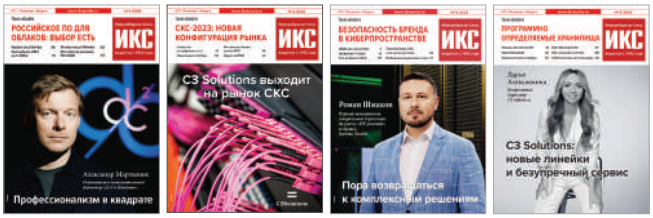
PDU комплектации Classic и Function, кроме того, оснащены портами для подключения дополнительных датчиков (дыма, утечки воды, открытия/закрытия дверей), а также имеют функцию мониторинга каждой розетки. В PDU предусмотрена настройка оповещения и предупреждения о перегрузках по электронной почте и протоколу SNMP. Комплектация Function обеспечивает удаленное управление каждой розеткой.

Все модели оснащены универсальными розетками и системой фиксации кабеля. Допускают возможность установки автоматических выключателей для защиты от перегрузки. Тип входного разъема – IEC 309 с возможностью выбора длины кабеля. Мощность – 3680–22170 Вт. Рабочая температура – от 0 до 55°C. По желанию заказчика возможна окраска в различные цвета.

Распределители питания сертифицированы и отвечают российским и международным стандартам.

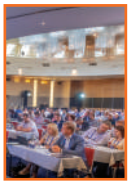
art-engineer.ru

ПЕРЕЧЕНЬ ПУБЛИКАЦИЙ-2023



КОЛОНКА РЕДАКТОРА / № 1–4

ИКС-ПАНОРАМА / № 1–4



ЭКОНОМИКА И БИЗНЕС / № 1–4

ИНФРАСТРУКТУРА / № 1–4

СЕРВИСЫ И ПРИЛОЖЕНИЯ / № 1–4

БЕЗОПАСНОСТЬ / № 1–4

РЕКЛАМА В НОМЕРЕ

Указатель фирм и организаций

Учредитель журнала «ИнформКурьер-Связь»:

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

МЕРОПРИЯТИЯ ИКС-МЕДИА

ИКС МЕДИА

2024

CLOUD & CONNECTIVITY 21.03

СКС. ЦОДы, офисы, общественные пространства 09.04

ЦОД: модели, сервисы, инфраструктура 25.04/17.06/26.11

Data Center Design & Engineering 21.05

ЦОД 2024 05.09

Data Center & Cloud Kazakhstan 08.10

Eurasia Data Center & Cloud Forum 05.11

Реклама/16+

География:
Москва
Санкт-Петербург
Новосибирск
Екатеринбург
Ташкент
Алматы

подробнее
на сайте iksmedia.ru

KEY POINT GROUP

РЕГИОНАЛЬНАЯ СЕТЬ ЦОД ГРУППЫ КОМПАНИЙ KEY POINT

ВАЖЕН КАЖДЫЙ!

ДАТА-ЦЕНТРЫ С СЕРТИФИКАЦИЕЙ TIER III

keypoint-group.ru