ТЕМА НОМЕРА

ВТОРАЯ КВАНТОВАЯ РЕВОЛЮЦИЯ

ИнформКурьер-Связь
ИКС
издается с 1992 года

EcoStruxure™
Innovation At Every Level

НАДЕЖНОЕ

решение для ИТ-провайдеров

Настенный сверхкомпактный 6U микро-ЦОД EcoStruxure™ от Schneider Electric™

- Компактная конструкция
- Быстрое развертывание
- Сокращение времени простоев и сервисных затрат

apc.com/edge

EcoStruxure™
IT Expert

Настенный сверхкомпактный 6U микро-ЦОД EcoStruxure™

Life Is On

APC by Schneider Electric

Издается с мая 1992 г.

Издатель
ООО «ИКС-Медиа»

участник
АНО КС ЦОД

Генеральный директор
Д.Р. Бедердинов
dmitry@iks-media.ru

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

Главный редактор

А.Г. Барсков
a.barskov@iks-media.ru

РЕДАКЦИЯ
iks@iks-media.ru

Ответственный редактор
Н.Н. Шталтовная
ns@iks-media.ru

Обозреватель
Н.В. Носов
nikolay.nosov@iks-media.ru

Корректор
Е.А. Краснушкина

Дизайн и верстка
Е.В. Денисова

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

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

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

Адрес редакции и издателя:
105066, Москва, ул. Новорязанская, д. 31/7, корп. 14
Тел./факс: (495) 150-6424
E-mail: iks@iks-media.ru
Адрес в Интернете: www.iksmedia.ru

№2/2020 подписан в печать 06.05.20.
Тираж 8 000 экз. Свободная цена.
Формат 64x84/8

ISSN 0869-7973

12+

Что будет с рынком ЦОДов

Сколько копий было в свое время сломано в дискуссиях о будущем дистанционных систем: обучения, медицины и пр. Сколько экспертов утверждали, что еще долго эти системы не получат в России серьезного распространения. Но вот прилетел «черный лебедь», и дистанционные системы стали использоваться повсеместно. Пандемия пройдет, а приобретенный положительный опыт останется, и спрос на эти системы и соответствующие услуги уже никогда не упадет до уровня, который был, когда мир еще не познакомился с COVID-19.

Хочется надеяться, что произошедшее – вынужденное введение режима самоизоляции и перевод работников на «удаленку» – заставит государство оперативно принять документы, упрощающие использование и реализацию дистанционных сервисов, в первую очередь телемедицины. Очевидно, что огромный стимул для развития уже получили системы дистанционного обучения, электронного документооборота, совместной работы, видеоконференцсвязи и пр.

Рост спроса на онлайновые сервисы подстегнул развитие облачных услуг. Мои коллеги из iKS-Consulting видят наибольший потенциал развития у облачных хранилищ данных, резервного облачного хранения и виртуальных десктопов. Согласно их прогнозу, аренда облачными провайдерами дополнительных мощностей в коммерческих ЦОДах позволит последним компенсировать недополученные из-за карантина доходы как от продаж услуг ЦОДов, так и от проектов миграции и инсталляции нового оборудования.

В соответствии с позитивным сценарием, разработанным в iKS-Consulting, ограничительные меры могут сократить выручку операторов коммерческих ЦОДов на 250 млн руб. Но аренда дополнительных площадей для развития облачных услуг даст дополнительно порядка 230 млн руб. Таким образом рынок ЦОДов «не заметит» кризиса и продолжит свое развитие со среднегодовым показателем роста на уровне 10–15%.

Но есть и негативный сценарий. Согласно этому сценарию, строительство новых ЦОДов будет массово сворачиваться, реализация многих ИТ-проектов отложится, а секвестирование или заморозка финансирования программы «Цифровая экономика РФ» отодвинет на несколько лет государственные проекты, включая внедрение ГЕОП. В результате рынок коммерческих ЦОДов вместо ежегодного 10–15%-ного роста войдет в фазу стагнации, а его реальное восстановление начнется лишь через несколько лет, в 2023–2024 гг.

С надеждой на позитивный сценарий,
Александр Барсков

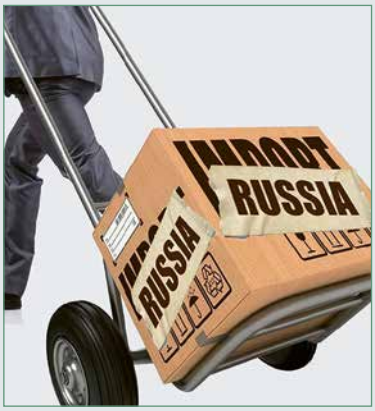
ТЕМА НОМЕРА

Вторая квантовая революция

с. 24

с. 4

Новые ЦОДы от атомщиков



с. 8

Г. Сизоненко. Это вредное слово «импортозамещение»

А. Барсков. Охлаждение ЦОДа: погружение неизбежно

В. Мосеев. Российские сети LPWA набирают абонентов

COVID-19 и ЦОДы: минимизация рисков на критических объектах

Новые ЦОДы от атомщиков

«Росэнергоатом» увеличивает присутствие на рынке дата-центров. В ближайших планах концерна – запуск ЦОДа в Казани и строительство крупных ЦОДов в Москве и Санкт-Петербурге.

«Построив крупнейший в Европе гиперЦОД “Калининский” (4800 стоек), мы поняли, что нет смысла останавливаться. Мы научились создавать коммерческие решения с облаками, в том числе российскими, и теперь рассматриваем дата-центры как бизнес. В качестве краткосрочных целей обозначили строительство трех центров обработки данных», – заявил заместитель генерального директора – директор по экономике и финансам концерна «Росэнергоатом» Сергей Мигалин.

В прошлом году «Росэнергоатом» (входит в электроэнергетический дивизион госкорпорации «Росатом») подписал с правительством Татарстана соглашение о строительстве ЦОДа на 500 стоек в Иннополисе. Сейчас идут проектирование и привязка к площадке, на которой в течение полугода начнется строительство. Отвечающая в концерне «Росэнергоатом» за продвижение и коммерциализацию дата-центров компания «Консист – Оператор связи» стала резидентом Иннополиса и открыла в городе филиал.

На стадии проработки находится проект строительства крупного (более тысячи стоек) ЦОДа в Москве. Еще один дата-центр (тоже на тысячу стоек) планируется развернуть в Санкт-Петербурге или его ближайших окрестностях.

ЦОД «Калининский» – крупнейший в Европе

Кроме того, в столице «Росэнергоатом» намеревается построить на площадке ВНИИАЭС и менее крупный ЦОД для увеличения вычислительных мощностей своего кризисного центра.

Компания продолжает политику строительства дата-центров рядом с атомными электростанциями. Дата-центр «Калининский» в Удомле обеспечивает электроэнергией Калининская АЭС. ЦОД в Иннополисе будет снабжаться Балаковской АЭС. Рядом с Санкт-Петербургом находится Ленинградская АЭС, электроэнергия в новый ЦОД может поступать и с Кольской АЭС. Планируется,

С. Мигалин: «Для нас принципиально важно создать географически связанный кластер Москва – Удомля – Санкт-Петербург»

что дата-центр в Санкт-Петербурге будет удовлетворять потребности предприятий Северо-Западного федерального округа, включая обеспечение функционирования Северного морского пути, а также поддерживать работу АЭС «Ханхикиви» в Финляндии, которую предполагается запустить в 2028 г.

Строительством ЦОДов «Росэнергоатом» занимается с 2015 г. Выгоды размещения дата-центров вблизи АЭС – прямое подключение к атомной станции, не подверженное технологическим рискам передачи электроэнергии по промежуточным сетям, использование систем защиты атомных станций, низкая стоимость электроэнергии.

Сначала «Росэнергоатом» создавал опорные дата-центры для развертывания и эксплуатации своих атомных станций. Летом 2017 г. концерн заявил о планах создания гиперЦОДа в Удомле, а в 2018 г. запустил его в эксплуатацию. Якорным партнером ЦОДа «Калининский» в Удомле выступает «Ростелеком», который арендует четыре пятых мощностей. Половину из оставшихся 800–1000 стоек используют «Росэнергоатом» для своих нужд и другие его клиенты, заполнение минимум еще одного зала на 200 стоек – задача 2020 г.

«С конца 2017 г. мы поняли, что не сможем ограничиться собственным потреблением, так как наши зарубежные заказчики – Турция, Египет, Бангладеш и в какой-то степени Узбекистан – проявили интерес к нашим решениям для создания национальных центров обработки данных», – отметил С. Мигалин. Концерн задумался о строительстве коммерческих ЦОДов за рубежом: дата-центр в Иннополисе станет референтным ЦОДом для дата-центра, который предполагается открыть в Турции.

Николай Носов

Время «больших»: M&A на рынке коммерческих ЦОДов

Бизнес коммерческих дата-центров в последние несколько лет заметно укрупнился.

По состоянию на конец 2019 г. Synergy Research Group насчитала в мире 348 сделок общим объемом $75 млрд. TMT Finance пишет о 31 сделке в минувшем году общим объемом $30 млрд.

Более трети всего объема сделок связаны с крупнейшими глобальными операторами дата-центров Equinix и Digital Reality (по оценкам Synergy Research Group, на их долю пришлось более 30% всех сделок на рынке). К крупным сделкам можно отнести приобретение американским оператором дата-центров Digital Reality нидерландской Interxion за $8,4 млрд с учетом долгов последней (через обмен акциями). К концу октября 2019 г. под управлением Interxion находились 53 ЦОДа в 11 европейских странах и 13 городах, включая Франкфурт, Амстердам и Париж. Эта сделка позволила Digital Realty увеличить количество ЦОДов до более чем 260 в 20 странах.

Анализ сделок подтверждает рост интереса к инвестициям в дата-центры и со стороны институциональных инвесторов. Почти половина объема всех сделок в сегменте ЦОДов пришлась на инвестиционные фонды private equity.

Среди потенциально крупнейших сделок институциональных инвесторов – намерение шведского инфраструктурного фонда EQT приобрести EdgeConneX (шт. Вирджиния, США) за $2,5 млрд (ведутся переговоры). Компания EdgeConneX основана в 2009 г., управляет 43 дата-центрами, имеет планы расширения в Европу.

Другой пример – американский фонд инфраструктурных инвестиций Digital Colony, который через свою портфельную компанию Vantage Data Centers (управляет дата-центрами в шт. Вирджиния, США) вышел на европейский рынок посредством приобретения компании Etix Everywhere. Таким образом, компания будет присутствовать в 11 странах. Vantage планирует инвестировать в свою европейскую экспансию около $2 млрд.

Другой американский фонд инфраструктурных инвестиций – Brookfield Infrastructure Partners – вышел на рынок дата-центров совместно с Digital Reality. Партнеры создали СП для приобретения бразильского дата-центра Ascenty за $1,8 млрд. Brookfield вложил $613 млн, получив приблизительно 49% уставного капитала совместного предприятия, которое владеет и управляет бразильским дата-центром.

В 2019 г. европейский фонд Asterion Industrial Partners подписал с Telefónica соглашение о намерениях приобрести 11 из ее 23 дата-центров за €550 млн. В периметр сделки не вошли серверы Telefónica, используемые компанией для собственных нужд и предоставления услуг клиентам. Telefonica будет продолжать оказывать весь перечень услуг, в том числе с использованием инфраструктуры 23 дата-центров, включая те 11, которые выставлены на продажу.

Южнокорейская Shinhan Investment Corp. затратила порядка $162 млн в рамках сделки с AMP Capital общим объемом $763 млн на приобретение американской компании Expedient (управляет 11 дата-центрами в США, предоставляет услуги ЦОДов и облачных вычислений).

Региональная экспансия операторов дата-центров через слияния и поглощения, в том числе с участием институциональных инвесторов, уже стала эффективной стратегией для многих игроков рынка, а укрупнение глобального рынка дата-центров – логичным этапом его эволюции.

Тенденция укрупнения коммерческих ЦОДов наблюдается и в России. «Ростелеком» уже на протяжении нескольких лет занимается покупкой наиболее привлекательных активов. Благодаря ряду приобретений общим объемом 25,1 млрд руб. (без учета чистого долга) компания стала крупнейшей на рынке коммерческих ЦОДов с долей почти 26%.

Ожидается, что тенденция укрупнения ЦОДов продолжится, небольшие и средние игроки будут постепенно «вымываться» с рынка. Способствовать «вымыванию» будет то обстоятельство, что многие коммерческие дата-центры были построены в 2000-х годах. Срок эксплуатации инженерного оборудования ЦОДа составляет примерно 10 лет, поэтому многим дата-центрам потребуется модернизация. Для операторов ЦОДов, имеющих единственную площадку, это может стать серьезной проблемой.

А значит, чтобы сохранять конкурентоспособность, нужно постоянно расширять свои мощности, строить и развивать новые площадки. Либо готовиться к «выходу» с рынка и искать покупателя на свой актив.

Татьяна Толмачева,
партнер, iKS-Consulting

НОВОСТИ ОТРАСЛИ

Облако «МегаФона»

«МегаФон» запустил в коммерческую эксплуатацию собственную платформу «МегаФон Облако». Платформа реализована на базе двух дата-центров в Москве, сертифицированных по стандарту TIER III Operational Sustainability, и аттестована по требованиям информационной безопасности в соответствии с ФЗ-152 по уровню УЗ1 и требованиям по информационной безопасности, предъявляемым к государственным информационным системам, по уровню К1. Благодаря использованию импортозамещающего оборудования и ПО платформа «МегаФон Облако» позволяет решать задачи не только крупного бизнеса, но и заказчиков из госсектора. Георезервирование между двумя ЦОДами гарантирует высокую отказоустойчивость платформы, а также дает возможность реализовывать различные сценарии обеспечения бесперебойной работы ИТ-систем заказчиков.

ЦОДы «Ростелекома» идут на восток

«Ростелеком» планирует в 2020 г. открыть центр обработки данных в Новосибирске, а в дальнейшем строить дата-центры на Дальнем Востоке и Юге России, сообщил первый вице-президент компании Владимир Кириенко. «Мы исходим из потребностей бизнеса: как правило, емкость стандартного ЦОДа регионального масштаба составляет 400 стойко-мест», – добавил топ-менеджер. Как говорится в материалах «Ростелекома», в 2019 г. выручка компании от услуг ЦОДов и облачных сервисов выросла на 50%.

ЦОД узнает свой персонал в лицо

Концерн «Росэнергоатом» провел пилотные испытания и готовит к коммерческому запуску систему биометрического видеоконтроля доступа к внутренним объектам своего опорного дата-центра при Калининской АЭС.

Система построена на базе сети видеонаблюдения внутри аппаратных залов ЦОДа, которая подключается к интеллектуальной цифровой платформе. Система фиксирует лица подходящего к оборудованию персонала, сверяет с действующей биометрической базой и подает оповещение оператору, если рядом с серверной стойкой находится неавторизованное лицо. Распознавание происходит за доли секунды с доказанной точностью в 99%.

Система распознавания лиц сейчас используется в зонах, где располагается серверное оборудование «Росэнергоатома». В скором времени услуга будет доступна и для коммерческих клиентов ЦОДа «Калининский».

ЦОД в Якутске

В Министерстве инноваций, цифрового развития и инфокоммуникационных технологий Якутии сообщили о договоренности с «Ростелекомом» по размещению современного ЦОДа уровня Tier III в центре Якутска. Реализация проекта начнется в 2020 г. Новый ЦОД будет предоставлять все основные услуги коммерческих дата-центров. По словам Анатолия Семенова, министра инноваций, цифрового развития и инфокоммуникационных технологий региона, изначально рассматривался вариант строительства ЦОДа на территории опережающего развития «Якутия» (в 40 км от Якутска). Позднее анализ потенциальных потребителей показал, что существует большой спрос на услуги дата-центра в самом Якутске.

SberCloud и Huawei – стратегические партнеры

Компании SberCloud, оператор облачной платформы группы Сбербанк, и Huawei договорились о стратегическом партнерстве, в рамках которого российским и зарубежным пользователям станет доступно облако SberCloud. Advanced. Новая облачная платформа имеет российскую юрисдикцию и размещается в облачной инфраструктуре компании SberCloud. Она ориентирована на крупный, средний и малый бизнес, а также на небольшие стартапы. Пользователям SberCloud.Advanced будут предложены 37 облачных сервисов, в том числе сервисы работы с кластерами больших данных и облачной контейнеризацией.

Новосибирск: ЦОД на 2,5 тыс. стоек к 2023 г.

Первое здание ЦОДа на 2,5 тыс. серверных стоек появится в Новосибирске к 2023 г., сообщил заместитель генерального директора компании «Нэолайн» Александр Суслов. До конца 2021 г. планируются разработка проекта и подготовка участка. В 2022–2023 гг. будут построены офисное и первое технологическое здания на 2,5 тыс. стоек. К 2024 г. компания намеревается возвести еще одно технологическое здание и к 2025 г. оснастить его оборудованием и инфраструктурой. Предполагается, что общий объем инвестиций составит 4,5 млрд рублей. Инвестор планирует окупить проект в 2028 г.

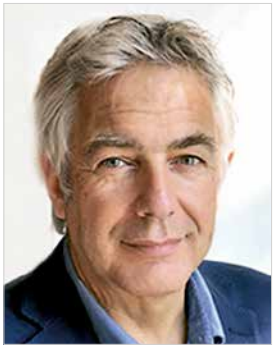
ИТ-компании попросили отнести их к числу наиболее пострадавших от кризиса

Ассоциация предприятий компьютерных и информационных технологий, среди членов которой компании «1С», ABBYY, Acer, IBM, «Лаборатория Касперского» и др., обратилась к Минкомсвязи России с просьбой включить ИТ-индустрию в перечень отраслей, наиболее пострадавших от пандемии коронавируса и экономического кризиса. Отсутствие поддержки может привести к банкротству ИТ-компаний, что негативно скажется на других отраслях, предупредили они.

ЦОДы в условиях пандемии

Критически важные объекты в условиях пандемии сталкиваются с особыми трудностями, как из-за возможного отсутствия ключевых сотрудников по причине болезни или карантина, так и в силу других факторов, которые могут повлиять на способность оператора поддерживать непрерывную работу объекта. Эксперты Uptime Institute предложили рекомендации, которые помогут операторам ЦОДов противостоять воздействию коронавируса, а также разработать стратегии и процедуры на случай эпидемических ситуаций в будущем.
Подробнее – на с. 80.

КОЛОНКА ЭКСПЕРТА



ЭНДИ ЛОУРЕНС,
исполнительный директор по исследованиям,
Uptime Institute

ОТКАЗЫ ЦОДОВ СТАНОВЯТСЯ ВСЕ БОЛЕЕ ПРОДОЛЖИТЕЛЬНЫМИ

Фиксируемое Uptime Institute увеличение числа продолжительных простоев ЦОДов эксперты связывают с усложнением ИТ-систем. Сбои в их работе могут оказаться гораздо более трудными для диагностики и устранения, чем отказы инженерной инфраструктуры.

Один из выводов недавно опубликованного доклада Uptime Institute Annual Outage Analysis 2020 заключается в том, что наиболее серьезные категории отказов в работе ЦОДов — те, которые ведут к значительным сбоям в предоставлении ИТ-сервисов, — вызывают все более тяжелые последствия и обходятся все дороже. Это неудивительно: как частные лица, так и предприятия становятся все более зависимыми от ИТ, и развернуть или заменить тот или иной ИТ-сервис делается все сложнее.

Другой вывод вызывает как вопросы, так и новые опасения: если отбросить те отказы, которые приводили только к частичной потере сервисов и оказывали минимальное влияние на их предоставление, то серьезные перебои, о которых публично сообщали операторы за последние три года, становятся все более продолжительными. А это, в свою очередь, является одной из причин того, что стоимость и тяжесть последствий отключений постоянно растут.

В таблице приведены собранные Uptime Institute за 2017—2019 гг. данные о случаях отказов, о которых сообщалось публично, за исключением тех, которые не повлекли за собой финансовых потерь, не сказались на конечных потребителях или причины которых не были установлены. Цифры свидетельствуют, что число сбоев растет. Это обусловлено рядом факторов, в том числе более широким развертыванием ИТ-сервисов и улучшением отчетности. Но они также показывают тенденцию к увеличению продолжительности отключений, особенно в категории более 48 ч (и это при том, что в выборку не вошла одна из главных причин длительных отключений – кибератаки с использованием программ-вымогателей).

Количество перебоев разной продолжительности в работе ЦОДов
(n – общее количество ЦОДов) ▼

Продолжительность, ч	2017 (n = 57)	2018 (n = 71)	2019 (n =140)*
0–1	1	4	20
1–4	35	25	49
4–12	13	25	26
12–24	4	6	14
24–48	2	4	14
>48	2	7	17

*Не включены перебои, причина которых неизвестна

Указанные в таблице интервалы – это время полного восстановления доступности ИТ-сервисов. Восстановление же поддерживаемых этими сервисами бизнес-операций может требовать больше времени, например, чтобы переместить самолеты туда, где они должны быть, или ликвидировать задержки в страховых выплатах. Эта тенденция не бросается в глаза, однако она реальна, что вызывает беспокойство, поскольку 48-часовой перерыв для многих организаций может стать смертельным.

Почему это происходит? Основные причины – сложность и взаимозависимость ИТ-систем, а также большая зависимость от программного обеспечения и данных. Так, исследования Uptime Institute показывают, что за последнее время все меньше серьезных отказов вызывается сбоями электропитания в ЦОДах и все больше – неполадками в конфигурациях ИТ-систем. Хотя решение технических проблем, связанных с инженерной инфраструктурой объекта, может быть непростым, обычно это относительно предсказуемая задача: отказы, как правило, однозначно определяются, процессы восстановления отработаны командой эксплуатации, а запасные части хранятся под рукой. Сбои в работе ПО, нарушение целостности данных и прерывание бизнес-процессов, охватывающих несколько организаций, могут быть гораздо более сложными проблемами – не только для решения, но даже для диагностики, и эти типы отказов становятся все более распространенными (и да, порой они вызваны именно отказом систем электропитания).

Какие уроки здесь можно извлечь? Основной вывод заключается в том, что методы обеспечения отказоустойчивости, наработанные службами эксплуатации ЦОДов за три с лишним десятилетия, нуждаются в расширении и интегрировании в сферы ИТ и DevOps и должны полностью поддерживаться и финансироваться руководством. Другой существенный вывод состоит в том, что аварийное восстановление как разновидность коммерческого сервиса, видимо, постепенно сходит со сцены, но сами принципы бдительности, восстановления и отказоустойчивости – особенно в условиях стресса – важны как никогда.

Это вредное слово «импортозамещение»

Григорий Сизоненко,
генеральный директор, ГК «ИВК»

Термин «импортозамещение» надо изъять из нашего лексикона: он дезориентирует и отрасль ИТ, и потребителей, и руководство страны. Я против импортозамещения в сфере информационных технологий! Но за технологическую независимость.

С конца восьмидесятых мы наблюдаем, как государство вкладывает деньги в госпрограммы, названия которых начинались раньше со слова «электронная», а теперь со слова «цифровая». С неизменным посылом: это электронно-цифровое (государство, производство, здравоохранение и т.п.) выведет страну на новый уровень технологического развития. За два десятилетия реализации подобных госпрограмм в стране создали множество различных информационных систем для решения прикладных задач. В них используются как зарубежные компоненты (SAP, Oracle), так и российские («1С», «Галактика» и др.). Например, автоматизировали МФЦ, создали ГИС «Госуслуги», ГАС «Правосудие», «Управление» и т.д. Дело полезное, нет сомнений. Но во всем многообразии уже построенных или строящихся систем есть принципиальный изъян.

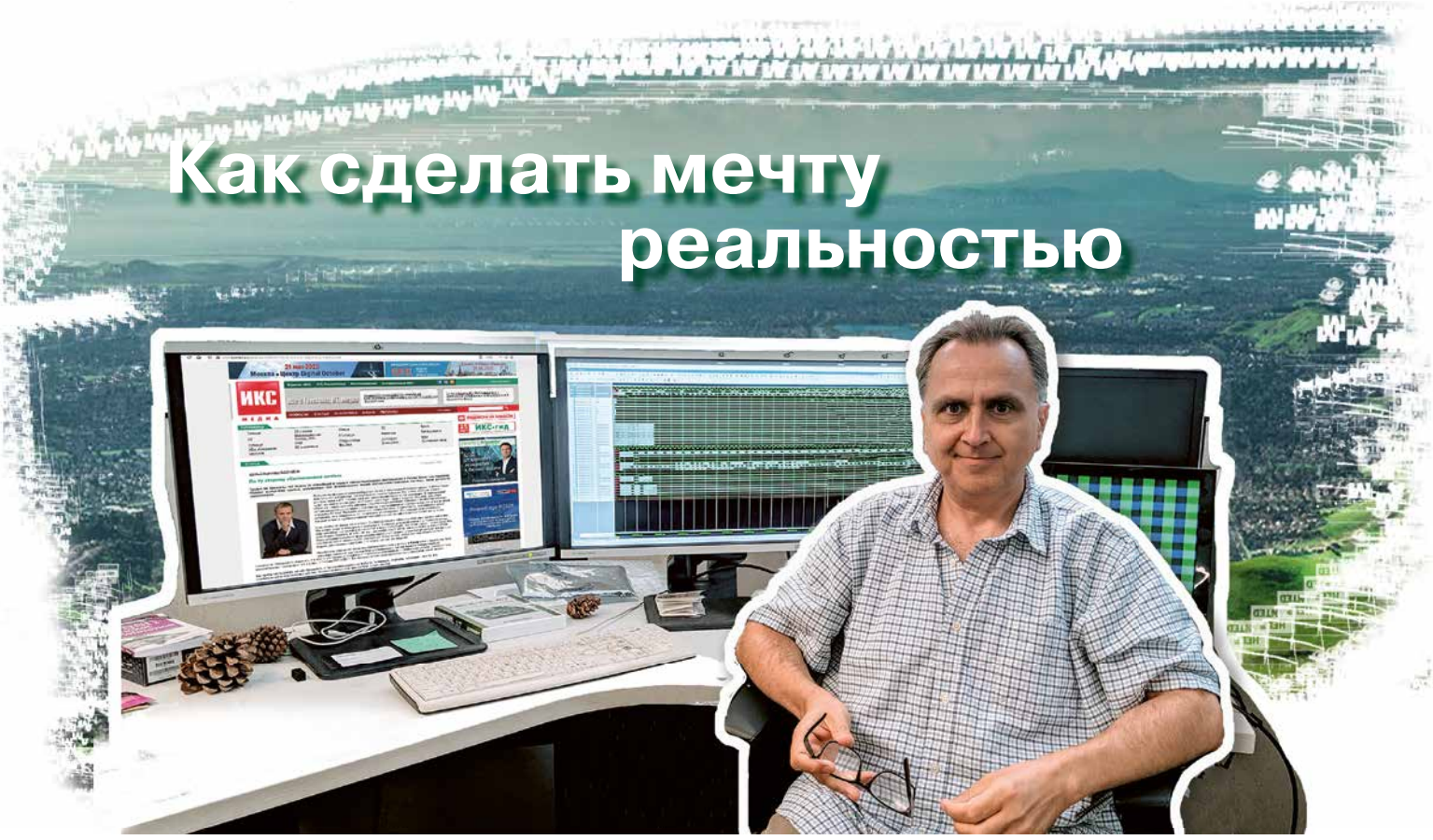
Тысячи информационных систем цифровой среды нашей экономики, науки, образования, медицины, социальной сферы практически целиком базируются на компьютерах с импортными процессорами Intel и импортной операционной системой Microsoft. Понятно, почему такой подход практиковали с девяностых до 2013 г. Но беда в том, что и теперь импортозамещающие прикладные системы строятся все на том же импортном фундаменте. Почему люди, ответственные за реализацию государственных планов в ИТ, этого не замечают? На мой взгляд – именно потому, что государство в лице огромной армии чиновников всех рангов декларирует стратегию импортозамещения, а не стратегию технологической независимости. Кстати, бывший вице-премьер высказывал мысль о том, что «Стратегию развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года» надо актуализировать. Она не соответствует вызовам времени. Но по сей день этого не сделано. Если мы продолжим цифровизацию в том же духе, мы будем ввергать себя во все бóльшую зависимость от зарубежных вендоров. Ни о каком выходе страны на новый уровень технологического развития речи не пойдет.

Настаиваю на том, что для сферы информационных технологий термин «импортозамещение» неправильный и даже вредный. Он открывает для недобросовестных чиновников, разработчиков и заказчиков заманчиво легкий путь. Заменил импортное приложение на отечественное – и ты молодец, участник большого государственного дела. Заменил еще парочку – вообще герой. Термин «импортозамещение» позволяет манипулировать понятиями, произносить патетические речи о пользе для государства, а на деле наносить ему вред. Вкладывать деньги в пафосные «надстроечные» проекты – и усиливать нашу зависимость в части фундамента.

Вот совсем свежий пример. В начале марта 2020 г. Совет по государственной поддержке создания и развития научных центров мирового уровня утвердил список из семи ключевых направлений, по которым до 2023 г. будут созданы девять таких научных центров. В итоговый список приоритетных направлений, в числе прочих, вошли передовые цифровые технологии, искусственный интеллект, роботизированные системы и материалы нового поколения, интеллектуальные транспортные и телекоммуникационные системы, высокотехнологичное здравоохранение, а также технологии обеспечения национальной безопасности. И опять – ни слова о том, на какой технологической базе (ОС и процессоры) будут работать все эти инновации. Кто может гарантировать, что они будут разрабатываться под отечественные операционные системы и процессоры, а не под продукты Intel и Microsoft? Ведь государство по-прежнему не обозначило ориентиры. Системные технологии по-прежнему не упоминаются в основополагающих документах по импортозамещению в ИТ. Откройте, например, «Стратегию развития отрасли информационных технологий в Российской Федерации» или национальную программу «Цифровая экономика Российской Федерации». Эти документы недвусмысленно демонстрируют, что Россия в принципе не рассматривает себя как производителя и поставщика информационных технологий. С таким подходом страна и дальше будет оставаться крупнейшим дистрибьютором и потребителем американских ИТ.

Строя планы развития информационно-коммуникационных технологий, мы должны ставить цель обеспечить технологическую независимость страны. Законодательно-финансовая активность государства, которая сейчас сконцентрирована на программной «надстройке», должна быть в первую очередь направлена на поддержку фундаментальных компонентов цифровизации – российских процессоров, российского системного ПО и собственной инфраструктуры разработки. Призываю всех – руководителей государства, госчиновников, разработчиков отечественных технологий, потребителей – осознать суть задачи, стоящей перед всеми нами. И от импортозамещения перейти, наконец, к обеспечению технологической независимости в ИТ. ИКС

Как сделать мечту реальностью



Юрий Панчул

Только последовательное увеличение глубины владения технологиями, как в образовании, так и в промышленности, позволит России добиться успеха на мировом рынке high-tech и в действительности построить цифровую экономику.

Я работаю в Кремниевой долине почти 30 лет и много раз наблюдал именно то паломничество из России, о котором пишет Игорь Бакланов в статье «По ту сторону “Силиконовой мечты”»*. Попытаюсь объяснить, почему этот процесс принес меньше, чем ожидали паломники, а также поделюсь одной историей, которая происходила без фанфар, но дала конкретный результат.

СПРАВКА ИКС

Юрий Панчул – проектировщик сетевых микросхем, автор и непосредственный участник ряда российских образовательных программ по микроэлектронике, основатель стартапа в Кремниевой Долине и инициатор русского издания учебника Дэвида и Сары Харрисов «Цифровая схемотехника и архитектура компьютера».

О чем мечталось?

Одна из черт человеческой психологии – это внимание к информации, которую легко переварить, и игнорирование непонятного. Поэтому всегда есть соблазн сосредоточиться на том, чтобы усвоить понятное, например организацию инкубаторов-акселераторов или классы акций и раунды инвестирования стартапа, и не обращать внимания на непонятное, скажем, на проектирование микроархитектуры сетевого чипа.

Так и паломники в Кремниевую долину с большим удовольствием посещали офисы Google и Facebook, а также выступления партнеров венчурных фондов. Поэтому за последние 10 лет в России переняли внешний вид офисов и процедуры инвестирования. Офисы в Сколково и у «Яндекса» выглядят не хуже, чем у Google, и лучше, чем штаб-квартира Intel. Российские венчурные инвесторы, их эксперты и консультанты растолкуют все про раунды финансирования и конвертируемые долговые обязательства не хуже, чем их коллеги из Пало-Альто.

Помогают ли эти ноу-хау выиграть на мировом рынке технологий? К сожалению, нет. Офисные здания технопарков сами по себе на успех влияют слабо. Многие стартапы в Кремниевой долине начинались в весьма заурядно выглядевших офисах, где их соседями были зубные кабинеты и другие традиционные бизнесы. Что касается ноу-хау инкорпорирования стартапов, обязанностей членов совета директоров и тонкостей обращения акций, то это любому основателю стартапа разъясняют за три похода к корпоративному юристу на деньги первого инвестора.

* И. Бакланов. По ту сторону «Силиконовой мечты». «ИКС» № 1'2020, с. 18.

Делали ли паломники серьезные попытки позаимствовать «тяжелые» ноу-хау, от обладания которыми стартапы, собственно, и выигрывают? Возьмем пример из области, во многом сделавшей Кремниевую долину Кремниевой, – из области проектирования полупроводниковых чипов. Автор статьи «По ту сторону...» вообще не упомянул о ней в своем описании «современных работников отрасли – от программиста до системного архитектора», поскольку системный архитектор, как правило, использует уже готовые чипы. Насколько за 10 лет России удалось продвинуться в этой сфере?

Степень заимствования тех или иных ноу-хау можно косвенно оценить по изданиям специализированной литературы. Недавно меня попросили высказать свое мнение относительно целесообразности перевода на русский язык нового издания книги о верификации цифровых чипов. Методы, которые описаны в этой книге, за последние 20 лет в Кремниевой долине стали использовать абсолютно все команды, проектирующие чипы, – от Intel, Apple, NVidia до Tesla, SpaceX и маленьких стартапов, разрабатывающих компьютеры для самоуправляемых автомобилей. Вывод пришлось сделать неутешительный: в России эта книга может заинтересовать 100–200 человек. Это на порядок или два меньше, чем в Кремниевой долине.

Что это значит? Представим себе, что некая страна решила вырастить у себя олимпийских чемпионов. Ее представители паломничают в другие страны, где перенимают технологии строительства красивых стадионов и фасоны спортивной формы, но не уделяют внимания физическим тренировкам спортсменов – бегу, упражнениям на брусьях и т.п., рассчитывая, что это устроится само собой. А потом жалуются, что спортсмены не выигрывают на олимпиадах.

Мечтать надо уметь

Но вот, скажем, американский историк науки Лорен Грэхэм из Массачусетского технологического института (MIT), которого регулярно приглашают на российские экономические форумы, считает, что с наукой и технологиями в России все в порядке и нашей стране не хватает лишь социального контекста и традиций продуктизации, превращения научных изобретений в айфоны и теслы. Следуя идеям Грэхэма и его коллег, российские паломники в Америку стали заимствовать у того же MIT именно ноу-хау в бизнесе и оставили безо всякого внимания другие ноу-хау, например, в области проектирования электроники.

Между тем в MIT с начала 2000-х годов есть базовый курс лабораторных проектов 6.111, который отлично помогает вырастить будущих проектировщиков чипов для айфонов и тесл. Упрощенный аналог этого курса есть в российских МИЭТ и ИТМО, но его стоило бы внедрить гораздо шире. Однако вместо этого стали перенимать умение делать слайды для презентаций инвесторам.

Год назад я присутствовал на робототехнической конференции в Сколково и обратил внимание на то, что бóльшая часть представленных проектов основывалась на довольно прямолинейном использовании готовых встраиваемых чипов. В самом факте нет ничего плохого – респектабельные производители холодильников в Айове или лазерных инструментов в Массачусетсе применяют микроконтроллеры примерно таким же способом. Но этого недостаточно для серьезного технологического прорыва на уровне экосистемы целой страны. Не хватает глубины и сложности, которые тяжело повторить и которые являются основой успеха Intel, NVidia и подобных им компаний.

Снова проведу аналогию. Представим, что мы взяли группу умных восьмиклассников, победителей всероссийских олимпиад по математике. С точки зрения средних взрослых они выглядят суперменами – могут быстро запрограммировать Arduino, построить нейросеть на NVidia или решить задачку по неэвклидовой геометрии. Посадим их в красивый офис, вручим миллионы долларов и придем к ним через год. Смогут они превзойти NVidia? Нет, они так и останутся на уровне Arduino и олимпиадных задач и не смогут конкурировать на внешнем рынке, потому что там им придется соперничать не со средними взрослыми и не с производителями, а с теми, кто углублял и оттачивал свои знания и умения сначала в университете, потом на опыте.

Без технической глубины даже упомянутая в статье Игоря Бакланова протестантская этика может сыграть злую шутку. В Кремниевой долине я не раз наблюдал, как вместо того, чтобы углубить свое понимание технологии, люди пытались приложить усилия к чему-то более простому. Например, компенсировали неконкурентоспособность по основному функционалу красивым графическим интерфейсом или маркетингом, поскольку не видели, как сделать собственно программу или устройство эффективными. Такие люди могут добросовестно и ответственно работать, но все равно проиграть на рынке и даже не осознать, почему это произошло.

Так что же делать? Последовательно увеличивать глубину владения технологиями, как в образовании, так и в промышленности. Снижать барьеры, расширять международные связи с университетами, поставщиками комплектующих для российских проектов и средств

проектирования. Одновременно вводить протекционистские меры для защиты внутреннего рынка от конечных продуктов из других стран, чтобы дать возможность развиваться российским компаниям, по крайней мере в некоторых нишах. Эксплуатировать все возможности, и на внешнем рынке, и на внутреннем, включая ниши, создаваемые импортозамещением. С увеличением глубины владения технологиями возможностей будет появляться больше.

Мечта, которая стала реальностью

Теперь о примере, внушающем оптимизм. Речь идет о «Байкал Электроникс», появившемся в 2012 г. дочернем предприятии суперкомпьютерной компании «Т-Платформы». «Т-Платформы» смогли пробить внешнеэкономический барьер и поставить спроектированные в России суперкомпьютеры в США. Компьютеры «Т-Платформ» были сделаны из готовых чипов иностранных производителей, но в новом проекте компания решила аккуратно увеличить техническую глубину, и «Байкал Электроникс» стала проектировать собственные чипы.

При этом «Байкал» не делал все с нуля, а заключил соглашения с тремя иностранными компаниями, лидерами в своих областях. Компания лицензировала процессорные ядра у британской ARM Holdings и у MIPS, американского отделения британской Imagination Technologies. У этих же компаний в свое время лицензировала блоки Apple (CPU – у ARM и GPU – у Imagination), скомбинировав их в чипах ранних айфонов со своими блоками.

Для проектирования системы на кристалле («чертежей» чипа) «Байкал Электроникс» использовала программы американской компании Synopsys, самого крупного в мире игрока в сфере автоматизации проектирования электроники, а для производства – фабрики тайваньской TSMC, которые точно так же используют и Apple, и другие компании.

Спроектированный московской командой «Байкал Электроникс» чип «Байкал-Т» был явлен миру в 2015 г., после чего его использовали в маршрутизаторах и управляющих компьютерах станков.

Этот проект соединил компании Кремниевой долины с Россией не конечными продуктами, а ноу-хау именно на уровне технологий проектирования. Это гораздо более серьезное достижение, чем усвоение российскими чиновниками искусства рисовать слайды в результате поверхностного паломничества в MIT и офисы Facebook.

Проект «Байкала» косвенно помог и другим российским проектам, в том числе MIPS-совместимому процессору из НИИСИ и спроектированным в России ядрам архитектуры RISC-V, которые идут глубже, в микроархитектуру процессорного ядра.

В качестве следующего шага «Байкал Электроникс» выпустила процессор «Байкал-М», совместимый с экосистемой ARM64. По производительности «Байкал-М» находится в одном классе с чипом MediaTek MT8173C, который стоит в ноутбуке Lenovo Chromebook C330. Это важный момент, поскольку за последние годы хромбуки с Chrome OS смогли занять рынок школьных компьютеров в США, отвоевав более 60% у компьютеров с Windows и MacOS. В результате для «Байкала» открываются новые перспективы, например, в создании школьного компьютера для России с Chrome OS от Google или даже со специальной версией ОС Linux, которая не требовала бы системного администрирования, возможно, в партнерстве с «Яндексом». Такой компьютер был бы прост и надежен, как телефон с Android. Предыдущие попытки внедрить Linux в российских школах не удались из-за сложностей техподдержки, но с фиксированной конфигурацией компьютера этих проблем можно избежать, как это получилось с Apple Mac и хромбуками.

Такая платформа создала бы возможности для производителей российских школьных и офисных программ. Из проблем стоит отметить стоимость чипов – в полупроводниковой экономике цены на чипы подобного типа могут быть низкими только при очень больших тиражах. Но это как раз тот случай, когда государству было бы выгодно дотировать первые партии компьютеров для формирования экосистемы и подготовки будущего прорыва. Проекту «Байкал» на ранней стадии государство помогало, финансируя его через «Роснано».

Таким образом, десять лет прошли не настолько зря, как утверждает автор статьи «По ту сторону “Силиконовой мечты”». Некоторые связи с Кремниевой долиной привели к появлению российских продуктов и формированию команд для следующих шагов. Хотя это не те связи, вокруг которых строится большая часть дискурса на многолюдных конференциях по стартапам и цифровому будущему со ссылками на Стива Джобса, Илона Маска и Лорена Грэхэма. ИКС

При поддержке

Минкомсвязь России

КООРДИНАЦИОННЫЙ СОВЕТ ПО ЦОДам И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ
Автономная некоммерческая организация

Спонсоры и партнеры

SberCloud · 3data Premium Data Centers · SUSE · CITRIX · Ростелеком ЦЕНТРЫ ОБРАБОТКИ ДАННЫХ · МегаФон · linxdatacenter · Selectel

Процессы решают все!

Дмитрий Аверьянов, независимый эксперт

По мере углубления цифровой трансформации люди в производстве товаров и услуг будут играть все меньшую роль, а процессы – все большую. Но эти процессы должны быть формализованы, стандартизованы, оптимизированы и хорошо управляемы.

Вездесущие процессы

О процессах в корпоративной управленческой среде говорят все больше: помимо давно вошедших в обиход бизнес-процессов, на слуху процессный подход, управление бизнес-процессами, и речь уже зашла о процессном офисе – выделенной структуре для управления бизнес-процессами.

Процессы, под которыми понимается совокупность взаимоувязанных действий, преобразующих некие входы (заготовки) в выходы (продукты или услуги), есть в любой компании. В противном случае эта компания ничего не производит – ни продуктов, ни услуг. Входы (заготовки), выходы (продукты), динамика преобразований, задействованные в них люди и роботы (программы), инструменты (ИТ-системы, рабочие места), документы, алгоритмы и т.п. – все это составляющие процесса. Даже в небольшой компании процессов очень много, и их можно детализировать, получая таким образом более мелкие процессы (подпроцессы).

Главная проблема – процессы невидимы, и точных инструментов их фиксации и идентификации пока нет (фотографирование рабочего дня, process mining и тому подобное картирование и логирование не являются точными). Если двум участникам одного процесса поставить задачу описать его, то чаще всего получатся два разных описания. Если нескольких топ-менеджеров попросить перечислить основные процессы в компании, ответы, скорее всего, будут разными – как по количеству, так и по названиям процессов. Этим и определяется специфика управления процессами: они, подобно рентгеновским лучам, насквозь пронизывают «тело» организации, но их нельзя увидеть или пощупать. Однако управлять ими нужно все равно.

Более того, эти невидимые процессы и есть основной актив компании. Известный лозунг «кадры решают все» сегодня трансформируется в «процессы решают все». Раньше приоритет кадров был справедлив, поскольку информация о процессе была сосредоточена в голове его исполнителя. Но со временем ситуация изменилась, например, в современном банкинге уровень автоматизации может превышать 99%, и роль человека в этом процессе стремится к нулю.

При повышении уровня автоматизации, переходе к «тотальной» цифровизации и далее к цифровой экономике процессам уделяется все больше внимания, а кадры как участник процесса отходят на второй план. Все больше и больше процессов принятия решений передается от человека к нечеловеку: набирают обороты технологии машинного обучения, искусственного интеллекта, роботизации бизнес-процессов, IoT и другие технологии цифровизации. Беспилотный автотранспорт, роботы коллцентров и т.п. выполняют свои процессы без участия человека.

Качество процессов и особенно их отчуждение от персоналий высоко ценил Генри Форд. Ему приписывают такую контрольную процедуру: неожиданно и срочно вызвать директоров своих заводов и изолировать их от управления, например, отправить в двухнедельный круиз по Карибскому морю. После этого американский автопромышленник смотрел, как работают заводы в отсутствие своих директоров. Если завод работал точно так же, как и с директором, то делался вывод, что процессы на заводе выстроены правильно, и директору давалась положительная оценка. Если же завод снижал производственные показатели, то его директора после круиза ждало увольнение, поскольку «ручное» управление считалось неприемлемым.

Развитие и усложнение процессов и бизнес-правил (правил принятия решений) привели к тому, что отдельный сотрудник знает логику процесса только на небольшом участке, а логику процесса в целом зачастую не знает никто. Если взять сквозной (кросс-функциональный) процесс, то даже специалист по методологии отдельно взятого функционального подразделения знает лишь свой участок.

Такую проблему как раз и устраняет процессный офис, он же офис управления бизнес-про-

цессами (Business Process Management Office, BPMO): он агрегирует отдельные участки в общий сквозной процесс и разграничивает зоны ответственности исполнителей. Задача BPMO не только формализовать процессы, создав соответствующие модели, в которых показать все взаимосвязи, параметры и свойства, но и осуществлять их мониторинг (измерение) с целью анализа процессов для дальнейшего их совершенствования и стандартизации.

Историческое отступление

Осознание значимости бизнес-процессов, точнее механизмов управления ими, росло постепенно. Процессный подход, ставший одним из ключевых элементов улучшения качества, сложился в 80-х годах прошлого века. Он дал толчок формированию выделенной дисциплины управления бизнес-процессами (Business Process Management, BPM) на основе средств автоматизации системной/программной инженерии (Computer-Aided System/Software Engineering).

Считается, что предложенная в 1992 г. Дэвидом Нортоном и Робертом Капланом сбалансированная система показателей (Balanced Scorecard, BSC) впервые пошатнула главенство финансовых индикаторов компании при оценке ее деятельности. Американские экономисты продемонстрировали, что нефинансовые показатели, ранее находившиеся в тени, прежде всего бизнес-процессы компании, не менее значимы. Также они доказали важность измерения процессов и взаимоувязку индикаторов эффективности (KPI), в том числе эффективности процессов, со стратегией предприятия.

Несмотря на успешность применения нерадикальных методов повышения эффективности, таких как lean, 6sigma и т.п., со временем пришло понимание, что существенные улучшения на каждом участке процесса не всегда обеспечивают столь же существенную оптимизацию процесса в целом. Взгляд на BPM как на инструмент революционного совершенствования бизнес-процессов был предложен в 1993 г. Майклом Хаммером и Джеймсом Чампи в концепции реинжиниринга бизнес-процессов, заложившей фундамент переосмысления и радикального преобразования бизнес-процессов компаний.

Сегодня концепция BPM получила мощный импульс благодаря цифровизации, которая рассматривается как цифровой реинжиниринг бизнес-процессов.

Три кита BPMO

Итак, процессный офис – это структурное подразделение компании, которое инвентаризует, формализует, систематизирует и стандартизирует бизнес-процессы компании, ведет их учет и мониторинг (измерение, сравнение, бенчмаркинг показателей) и участвует во внедрении новых процессов и совершенствовании текущих. Азбукой BPM/BPMO сегодня является «Свод знаний по управлению бизнес-процессами» (Business Process Management Common Body of Knowledge). Первая версия этой книги была выпущена в 2008 г. В 2018 г. приказом Минтруда России утвержден профессиональный стандарт «Специалист по управлению процессами». В некоторых отраслях утверждены собственные стандарты BPM, например, у Ассоциации российских банков есть Стандарт качества организации работы по управлению бизнес-процессами в кредитных организациях.

Рассмотрим основные документы, на которые опирается BPMO в своей работе. Первый из них – это реестр высокоуровневых процессов. Эталоном такого реестра принято считать классификатор процессов Американского центра производительности и качества (American Productivity & Quality Center Process Classification Framework, APQC PCF). Существуют универсальный вариант классификатора и ряд отраслевых. Однако ничто не мешает заимствовать из APQC PCF принципы классификации/систематизации процессов, но разработать свою версию реестра, учитывающую, например, организационно-штатную структуру компании или функциональную специализацию подразделений.

Обычно высокоуровневыми считают процессы, которые на выходе дают продукты компании, это так называемые продуктивные (продуктовые) процессы. Процессы этой группы имеют прямую связь с каталогом продуктов (услуг).

Вторым по значимости документом является матрица ответственности (Responsible/ Accountable/ Consulted/ Informed matrix, RACI), которая для высокоуровневых процессов позволяет сопоставить их владельцев и участников с подразделениями компании. Подобная RACI-матрица основывается на организационно-штатной структуре предприятия, поэтому древовидная структура объектов (процессов, подразделений) и фильтры облегчают навигацию от процесса к его участникам (владельцу, другим ролям из RACI-матрицы) и наоборот.

Топ-3 документов BPMO замыкает альбом схем процессов верхнего уровня. В нем собраны концептуальные схемы по всем направлениям деятельности компании. В отличие от реестра процессов (иерархическое дерево) и табличной формы RACI-матрицы, графическое

Процессный офис 1.0

Процессный комитет

Руководитель BPMO
Директор по процессам

Блок моделирования процессов	
Процессы «по-крупному» (процессы – «леса»)	**Процессы детально (процессы – «деревья»)**
▪ Ведение реестра, схем укрупненных процессов, портфеля процессов (статусы, владельцы и т.п.) ▪ Ведение RACI-матрицы (укрупненной) ▪ Контроль корпоративной архитектуры (бизнес- и технологический уровень) ▪ Ведение каталога продуктов (тарифов)	▪ Ведение общего каталога (возможно, вместе с оргштатной структурой, структурой ИТ-систем и т.п.) ▪ Моделирование (описание) процессов, верификация моделей, разработанных вне BPMO ▪ Имитационное моделирование процессов

Блок методологии и нормативных документов		
Общая методология	**Собственная методология**	**Архив нормативных документов (НД)**
▪ Координация бизнес-аналитиков сторонних подразделений или организация выделенного подразделения бизнес-аналитики ▪ Разработка и своевременная корректировка регламентов, инструкций, политик	▪ Разработка единой системы классификации и кодирования информации: кодов (процессов, продуктов, документов), справочников, классификаторов ▪ Создание регламентов BPM, деятельности BPMO, соглашений о моделировании, корпоративной библиотеки условных знаков ▪ Совершенствование технологий BPM, автоматизация BPMO	▪ Ведение нормативной базы компании (политик, регламентов, инструкций), документации на системы и процессы, норм-контроль НД ▪ Публикация процессной информации на корпоративном портале

Блок эффективности и аудита	
BSC/KPI	**Аудит BPMO**
▪ Анализ стратегий, целей, предложения по улучшению KPI, участие в стратегическом планировании ▪ Измерение процессов, мониторинг KPI и активности бизнес-процессов ▪ Интеграция с системами управления операционным риском компании	▪ Оценка зрелости процессов и процессного управления ▪ Взаимодействие со службами внутреннего контроля ▪ Подготовка обучающих материалов по BPM, обучение и тестирование сотрудников BPMO и компании, популяризация BPM в компании

Блок разработки и развития		
Цифровизация	**ИТ**	**Реинжиниринг**
▪ Исследование и внедрение технологий цифровизации, новых взглядов на продукты компании ▪ Реинжиниринг текущих процессов в направлении их цифровизации	▪ Проектирование инструментами класса «программирование без программирования», интеграция разработок в ИТ-ландшафт ▪ Глубинный анализ процессов ▪ Участие в построении корпоративной ИТ-архитектуры, привязка процессов к ИТ-ландшафту	▪ Анализ и оптимизация процессов собственными силами, включая подходы lean, 6sigma и т.п. ▪ Взаимодействие с проектным офисом с целью создания новых процессов, внедрения новых систем, оптимизации и модернизации

представление процессов интуитивно более понятно и позволяет на 100–200 листах показать «в крупную клетку», как работает компания в целом, какие процессы в ней существуют, как они связаны и кто их реализует.

Для многих отраслей разработаны детализированные эталонные модели бизнес-процессов, например, для телекоммуникаций – eTOM (enhanced Telecom Operations Map), для банков – BIAN (Banking Industry Architecture Network), для ИТ-процессов любой компании – ITIL (Information Technology Infrastructure Library).

Структура процессного офиса

BPMO должен стать центром компетенции по процессам компании: он осуществляет детальный учет процессов (аналогично бухгалтерскому учету), фиксацию текущего состояния и моделирование процессов, управление их изменениями, измерение и аудит, эволюционный «улучшайзинг» и революционный реинжиниринг, цифровизацию и т.п. На схеме показана развернутая конфигурация процессного офиса в версии 1.0. На практике процессные офисы включают обычно только часть указанных блоков.

Процессный комитет – это коллегиальный орган (стоящий над BPMO) с полномочиями, достаточными для координации деятельности владельцев процессов и принятия стратегических решений в части управления бизнес-процессами компании. Например, выделяется технологическая стратегия развития компании, которая опирается на бизнес-стратегию и содержит как один из своих элементов ИТ-стратегию компании.

Трехуровневая модель «бизнес – технология – ресурсы» включает в себя:

1) бизнес-слой;

2) слой процессных технологий: процессы и бизнес-ориентированные технологии (например, для банков – банковские технологии);

3) ресурсы (включая трудовые) и инструменты, включая информационные и другие инфраструктурные технологии.

Позаботьтесь о своих процессах, создайте для них BPMO, ведь процессы – самое ценное, что есть в компании, как ни тяжело это слышать сотрудникам, исполнителям пока не полностью автоматизированных процессов. При 100%-ной автоматизации / цифровизации на рабочем месте останутся только роботы, андроиды и т.п. и главный над ними – цифровой BPMO. ИКС

DCDE FORUM

ИКС МЕДИА

8-я международная конференция

DATA CENTER DESIGN & ENGINEERING

10 декабря 2020 • Москва • Центр Digital October

www.dcdeforum.ru

16+ Реклама

За дополнительной информацией обращайтесь по телефону: (495) 150-6424 и e-mail: dim@iksmedia.ru

При поддержке

Минкомсвязь России

При участии

КООРДИНАЦИОННЫЙ СОВЕТ ПО ЦОДам И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ
Автономная некоммерческая организация

Uptime Institute

Спонсоры и партнеры

Life Is On Schneider Electric

MITSUBISHI ELECTRIC Changes for the Better

VERTIV

RITTAL

СМАРТ КОНСТРАКШН #Sberbuild

ZEBC ЭЛЕКТРО

Janitza

C3 SOLUTIONS КАЧЕСТВЕННО.СДЕЛАНО.В РОССИИ.

CONTEG to complete your network

АККУ-ФЕРТРИБ

ИМПУЛЬС ИСТОЧНИКИ БЕСПЕРЕБОЙНОГО ПИТАНИЯ

Дом, который построит Сбербанк

Сбербанк, накопив экспертизу в проектировании и строительстве дата-центров, вышел на российский рынок создания сложных инженерных объектов.

Сергей Шуршалин

Публичное акционерное общество Сбербанк уже давно не банковская организация, и даже не «ИТ-компания с банковской лицензией», а экосистема бизнесов, связанных с крупнейшей финансовой организацией страны. Одно из новых направлений деятельности российского гиганта – строительство. В феврале прошлого года появилась дочерняя структура Сбербанка – компания «Смарт Констракшн», директор которой Сергей Шуршалин согласился ответить на вопросы нашего издания.

– Сергей Борисович, раньше Сбербанк привлекал для строительства своих дата-центров внешних генподрядчиков. Например, в проекте мегаЦОДа-2 Сбербанка в Сколково, победившем в наиболее престижной номинации «Проект года» профессиональной премии в области дата-центров Russian Data Center Awards, наряду с дочерней компанией Сбербанка «СБ Девелопмент» участвовал внешний генподрядчик. Почему теперь возникла идея создания своей компании с функцией генподрядчика?

– Компания «Смарт Констракшн» образована ради проекта создания технопарка ПАО «Сбербанк» в Сколково. Мы провели внешний конкурс по выбору генподрядчика на его строительство. В нем участвовало около десятка компаний – потенциальных генподрядчиков. К сожалению, никто из претендентов не смог сделать адекватного предложения, и конкурс не состоялся. В итоге правление Сбербанка приняло решение сформировать внутри своего департамента строительства компанию для создания технопарка – «Смарт Констракшн». Решение в тренде эволюции Сбербанка, который развивается как мультисервисная компания.

Технопарк в Сколково – многофункциональное пространство для комфортной работы, спорта и творчества. Концепция выбрана по итогам международного конкурса, победителями которого стали представители британского архитектурного бюро Захи Хадид. В здании технопарка будут находиться офисы Сбербанка, переговорные помещения, бизнес-инкубатор, клиентская зона, зоны питания, места для занятия спортом и йогой, отель и даже релакс-библиотека. Общая площадь технопарка – 270 тыс. кв. м. В десятиэтажном здании будут работать более 14 тыс. человек – в основном сотрудники Сбербанка из блока «Т» («Технологии»).

Постепенно развивались компетенции компании в генеральном проектировании, появлялись новые задачи. Сейчас «Смарт Констракшн» строит шестой блок мегаЦОДа Сбербанка в Сколково, проектирует огромный новый ЦОД на 70 МВт в Москве в Южном порту – шестиэтажное здание, расположенное на месте автостоянки первого мегаЦОДа. Помимо технопарка, для желающих работать в Сколково сотрудников мы возводим жилой комплекс.

– Сбербанк уже создавал компании, которые решали непрофильные для него задачи. Например, «Сбербанк Технологии» – это по сути инсорсинговая ИТ-компания для разработки ИТ-решений Сбербанка. «Смарт Констракшн» тоже нацелена исключительно на инсорсинг?

– Нет. Компания не только строит объекты для Сбербанка, но и работает с внешними заказчиками и ведет переговоры о создании инфраструктуры для них. Уже сейчас мы – полноценная строительная компания, которая может выполнять подряды крупных государственных структур и бизнеса, в том числе малого и среднего.

– Как организовано взаимодействие с другими подразделениями Сбербанка?

– У нас есть хештег #Sberbuild, который объединяет управляющий процессом на верхнем уровне департамент строительства Сбербанка и дочерние компании публичного акционерного общества: технического заказчика «СБ Девелопмент» и генподрядчика «Смарт Констракшн». Все три структуры могут работать как с внутренним потребителем, так и на внешнем рынке. Есть и производственные мощности, например, собственный завод металлоконструкций. Мы способны выполнять сложные внешние инфраструктурные заказы, строить не только ЦОДы, но и офисные и производственные объекты.

– Вы первыми в России построили мегаЦОД с полноценным фрикулингом. Хотя многие говорили, что в Москве из-за загрязненности воздуха этого сделать нельзя. Как оцениваете опыт использования данной технологии?

– Технология охлаждения нового ЦОДа в Южном порту пока обсуждается. Целесообразность применения фрикулинга зависит от конкретного проекта. Даже в Москве условия разные. В районе Рублевского шоссе часты туманы, в Сколково – постоянно меняющий направление сильный ветер. Хороший теплообмен и влажность предопределили использование фрикулинга в мегаЦОДе в Сколково. На востоке Москвы намного суше, нет ветра, воздух не перемещается. Надо учитывать много факторов – стоимость оборудования, фильтров для очистки воздуха, которые надо постоянно менять, а это влияет на

ТСО проекта. Забота об экологии – довод в пользу фрикулинга. Но и тут не все просто. Ведь фильтры необходимо утилизировать. Автомобиль Tesla не загрязняет воздух, но не надо забывать о нагрузке на экологию при производстве электроэнергии для него и утилизации батарей. Каждый случай выбора фрикулинга – частный, требующий анализа различных факторов.

– Какие новые технологии в строительстве ЦОДов вы могли бы выделить?

– Принципиально новых технологий пока, к сожалению, нет. Внимание специалистов направлено в основном на оптимизацию существующих решений, например, на повышение температуры в машзалах. Сейчас в новых ЦОДах нет необходимости охлаждать залы до 22°С, как это требовалось раньше, рабочая норма температуры эксплуатации ИТ-оборудования повысилась в среднем на 10°С.

Другой тренд – более широкое использование внутренних высоковольтных коммуникаций. Максимум дистрибуции на 10 или даже 20 кВ и только в конце линии – понижение напряжения посредством трансформатора, что позволяет ощутимо минимизировать потери электроэнергии и повысить эффективность энергопотребления.

– Какие принципы и стандарты компания использует при проектировании ЦОДов?

– Многолетний опыт создания и эксплуатации объектов критической инфраструктуры позволил сформировать крепкую профессиональную команду сотрудников, набрать собственную статистику, проанализировать международный опыт и лучшие практики. Все это дало нам возможность сформулировать собственные стандарты. Конечно, наши подходы к отказоустойчивости коррелируют со стандартами The Uptime Institute – уровень требований к нашим мегаЦОДам находится между Tier III и Tier IV. Мы также сами формируем более высокие требования к стандартизации залов, всегда оцениваем удобство и стоимость последующей эксплуатации объекта. Представители эксплуатационной службы подключаются к реализации проекта на самых ранних стадиях, и мы внимательно относимся к их рекомендациям. Учитываем возможность дальнейшей модернизации оборудования. Закладываем запас по месту и толщине подводимых шин, чтобы замена оборудования не приводила к дорогой реконструкции залов. Чтобы ЦОД служил как минимум 15 лет, и на протяжении этого срока за счет смены поколений поддерживалась возможность использования самого современного инженерного оборудования.

Накопленная экспертиза позволила создать в «Смарт Констракшн» полноценный проектный институт, в котором внедрены современные средства разработки, включая ПО для моделирования тепловых потоков, где применяются BIM-технологии, строятся 3D-модели объектов и проектируются все стадии возведения объекта вплоть до выпуска рабочей документации. Причем все системы моделируются в комплексе, что предотвращает конфликты и аварийные ситуации на стадии строительства и эксплуатации.

Еще один наш принцип – независимость от вендоров-монополистов. Для нас важно, чтобы любое реализуемое нами техническое решение было апробировано и представлено на российском рынке как минимум пятью разными производителями. К примеру, в ситуации с дизель-генераторами мы предпочтем три дизель-генератора по 1 МВт одному мощностью 3 МВт, потому что такие мощные ДГУ мало кто производит и найти их на рынке сложно. Да, на стадии проекта мы могли бы несколько сэкономить, купив одно устройство, но если анализировать возможные риски последующей эксплуатации или замены, то подобная экономия может обернуться серьезной проблемой в будущем и поставить нас в опасную зависимость от поставщика.

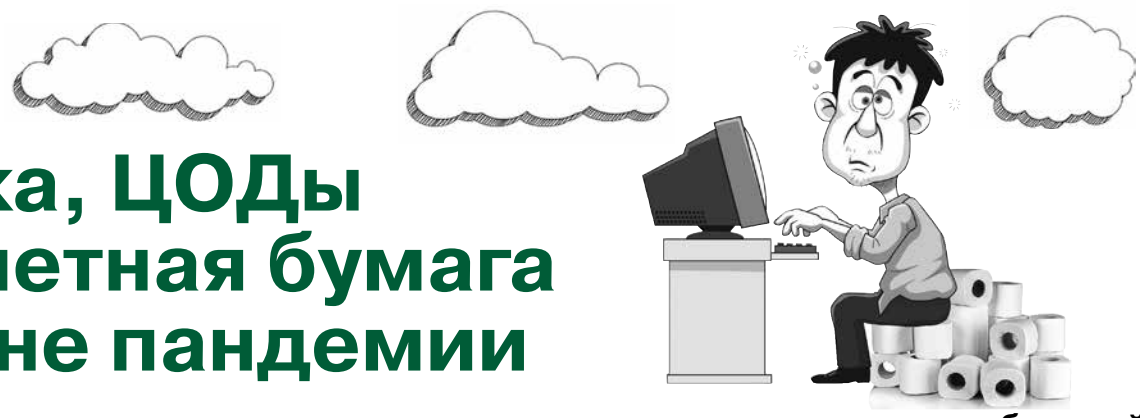
– Каковы преимущества у «Смарт Констракшн» на рынке?

– Прежде всего, мы являемся дочерней компанией Сбербанка и можем заниматься самофинансированием проектов. Можем работать по принципу: маленький аванс, а основная оплата – после закрытия работ. В современных условиях это ключевое преимущество на строительном рынке.

Наша команда накопила огромный опыт проектирования и строительства мегаЦОДа Сбербанка «Южный порт», мы использовали его при строительстве мегаЦОДа-2 в Сколково. Никто в России пока не делал столь масштабных проектов дата-центров. Причем у нас есть опыт не только проектирования и строительства, но и промышленной эксплуатации подобных объектов, когда на практике можно реально оценить правильность и эффективность тех или иных инженерных решений. И этот уникальный опыт тоже является нашим конкурентным преимуществом на рынке.

Объединяемые хэштегом #Sberbuild структуры Сбербанка сами проводят НИОКР, сами проектируют и сами выступают в качестве генподрядчика, привлекая субподрядчиков и контролируя их работу. При этом мы, являясь частью мощной многофункциональной структуры, имеем возможность оптимально использовать ее ресурсы и экспертизу для решения самых сложных и нестандартных задач при создании масштабных инфраструктурных объектов, требующих специализированных отраслевых знаний. Одним из важных примеров синергии наших внутренних ресурсов являются наши возможности в области физической безопасности и кибербезопасности. Специалисты разных департаментов совместно могут консолидировать требования к общестроительной, инженерной и информационной инфраструктуре с точки зрения соответствия российским, международным нормам и лучшим мировым практикам.

Подводя итог, хочу отметить, что для успешной реализации крупных инфраструктурных проектов генподрядчику необходимо иметь опыт, экспертизу, профессиональную команду менеджеров и исполнителей, а также доступ к необходимым финансовым ресурсам, которые зачастую являются базисом и ключом к успеху проекта.



Облака, ЦОДы и туалетная бумага на фоне пандемии

Николай Носов

Охватившая весь мир эпидемия коронавируса меняет глобальный рынок дата-центров и облаков.

Пандемия вызвала резкий рост спроса на онлайн-услуги. Компании переводят своих сотрудников на удаленную работу, школьники и студенты учатся через интернет, люди на самоизоляции заказывают доставку продуктов на дом, смотрят фильмы и осваивают стриминговые игры. Резко возросла нагрузка на облака, ЦОДы и телеком-компании. Телеком – одна из немногих отраслей, которая, по оценкам Gartner, выглядит оптимистично как в ближней, так и в дальней перспективе.

Ажиотаж в мире

Компания Microsoft в своем блоге заявила о том, что в районах, закрытых на карантин, потребление облаков Azure выросло на 775%! Впоследствии компания уточнила, что речь идет только о сервисе Microsoft Teams в Италии, но и эти данные впечатляют. Число пользователей Microsoft Teams в мире увеличилось до 44 млн, и за последнюю неделю марта у них в облаке состоялось 900 млн виртуальных контактов. За тот же период на 42% выросло использование средств визуализации данных Microsoft Power BI, предназначенных для предоставления официальной информации о COVID-19 гражданам. Переход на удаленную работу привел к трехкратному росту потребления услуги виртуального рабочего стола (Microsoft Virtual Desktop).

Компания Microsoft предприняла шаги по снижению полосы пропускания для онлайн-видео, попросила разработчиков игр выпускать обновления для сетевого сервиса Xbox Live в непиковое время, заявила, что ускоряет добавление больших объемов новых вычислительных мощностей, которые будут доступны в ближайшие недели.

Основатель компании – агрегатора облачных сервисов Cloudscene Беван Слаттери сравнил ажиотаж вокруг ЦОДов с неожиданным бумом покупок туалетной бумаги, когда в условиях неопределенности люди покупают намного больше, чем понадобится в ближайшее время. По его оценкам, из-за переходящих на работу в облако людей нагрузка на вычислительные мощности провайдеров уже возросла на 50–100% и возрастет еще на 100–200% в ближайшем будущем.

Компании пытаются получить все доступные мощности. Спрос значительно превышает предложение, что сказывается на ценах. «После того, как имеющиеся вычислительные мощности бу-

Влияние факторов, связанных с COVID-19, на инвестиции в технологии ▶

Отрасль	Краткосрочное влияние	Долгосрочное влияние
Банковский сектор и безопасность	Негативное ↓	Разнонаправленное ↔
Телеком	Позитивное ↑	Позитивное ↑
Образование	Позитивное ↑	Позитивное ↑
Госсектор	Позитивное ↑	Позитивное ↑
Здравоохранение	Позитивное ↑	Позитивное ↑
Страхование	Негативное ↓	Разнонаправленное ↔
Промышленность	Негативное ↓	Разнонаправленное ↔
Ритейл	Негативное ↓	Разнонаправленное ↔
Транспорт	Негативное ↓	Негативное ↓

Источник: Gartner

дут задействованы, потребуется 12–18 месяцев для ввода новых мощностей в эксплуатацию. В условиях ажиотажа операторам дата-центров придется нормировать мегаватты как туалетную бумагу. Прекрасное время для облачного бизнеса и дата-центров», – считает Беван Слаттери.

Облака карантинной России

Западные тенденции доходят до России с задержкой. Когда в Нью-Йорке сметали с полок магазинов туалетную бумагу, то в России делали только небольшие закупки «на всякий случай», да и то под воздействием телевизионных новостей из США. Тем не менее спрос на облачные услуги в стране вырос. Так, по данным компании GFN.RU, за первую неделю самоизоляции число ежедневно играющих с помощью стримингового сервиса пользователей увеличилось почти в три раза, а количество ежедневно регистрирующихся в сервисе клиентов – более чем в шесть раз. За восемь дней карантина суммарное игровое время пользователей компании составило 47 лет.

Стали использоваться минимизирующие контакты с персоналом облачные приложения, например облачная система заказа пропусков PASS24.online группы компаний ЛАНИТ, позволяющая заказывать пропуск через мобильное приложение, исключая личный контакт с охраной на КПП.

Пока неясно, как в этом году будет проводиться единый государственный экзамен для школьников, но «Мегафон» уже запустил на собственной образовательной платформе онлайн-курсы по подготовке к ЕГЭ с возможностью не только просматривать видеолекции, но и посылать выполненные задания на проверку.

Компания Huawei провела первую публичную онлайн-демонстрацию своего облака под зонтиком Sbercloud. На первый взгляд – очень похоже на AWS, так что пользователям облаков американского гиперскейлера и переучиваться не придется. «Под капотом» – проприетарное ПО китайского гиганта, разработанное на базе облачной платформы OpenStack, хорошо знакомой службам эксплуатации самого крупного российского банка.

Жизнь в российских облаках не замерла из-за карантина, нагрузка на облака и ЦОДы растет, но прогнозы делать трудно. С одной стороны, в ситуации неопределенности бизнес, которому требуется расширить ИТ-инфраструктуру, старается не вкладывать средства в долгосрочные проекты, а использовать модель аутсорсинга. Это стимулирует рост рынка ЦОДов и облаков. С другой стороны, кризис в экономике сокращает общее количество компаний, которым требуется расширение инфраструктуры, да и вообще количество компаний. Какой из этих трендов окажется сильнее, покажет время. Экономический кризис 2014–2015 гг. дал положительный импульс развитию ЦОДов и облаков.

«Коронавирусный» фактор, связанный с изоляцией большого количества сотрудников, накладывается на общий экономический кризис. Как раз компании, в которых развиты ИТ на стадии производства или управления, могут переходить на дистанционную работу. И делают это. В результате увеличивается востребованность различных облачных сервисов.

> Факторов, влияющих на развитие рынка ЦОДов и облаков в связи с эпидемией COVID-19, много, но они разнонаправленные.

Станислав Мирин, ведущий консультант, iKS-Consulting

Очевидно, что значительно возрастает нагрузка на российских телеком-операторов. Что касается российских облачных провайдеров, то надо подождать официальных отчетов. Ведь значительная часть нагрузки уходит в западные облака. Например, используются коммуникационные программы типа Skype, Zoom, WhatsApp. Тот же Microsoft Office 365, позволяющий выполнять совместную работу с документами или аналогичный пакет G Suite – это все зарубежные облачные продукты, не имеющие «приземления» у российских провайдеров.

Если оценивать рост отечественных облаков из-за пандемии в 30%, то при используемых сейчас в стране под облака 2000 стоек увеличение потребности составит 600 стоек. Это меньше 1,5% стоек, установленных сегодня в российских коммерческих дата-центрах. При этом часть облачных провайдеров на рынок коммерческих ЦОДов не выйдет, поскольку имеет свои резервы. Да и сам перенос вычислительных мощностей в коммерческие ЦОДы сдерживается сложностью работы в условиях карантина.

Другой негативный фактор – экономический кризис и спад активности бизнеса. Рост курса американского доллара не будет способствовать строительству новых ЦОДов и закупкам компаниями ИТ-оборудования, но, как и в случае скачков курса в прошлом, стимулирует использование вычислительных мощностей коммерческих ЦОДов, рублевые цены на которые будут увеличиваться с большой задержкой. «Вероятно, – заключает ведущий консультант аналитического подразделения iKS-Consulting Станислав Мирин, – мы увидим всплеск отложенного спроса после победы над вирусом, так как изменения в парадигму использования облаков он точно внесет». ИКС

Этический вектор современных ИТ. «Электронный концлагерь» или iGOELRO?

Игорь Бакланов

Отсутствие этического дискурса в профессиональном сообществе ученых и инженеров долгое время считалось нормой. Но с развитием ИТ, появлением симбиоза технологий, компьютеров и людей неизбежно приходится снова решать проблемы добра и зла.

– А меня ты боишься? – спросил Александр.
– А что ты такое, – спросил Диоген, – зло или добро?
– Добро, – сказал тот.
– Кто же боится добра?
…Наконец, Александр сказал:
– Проси у меня чего хочешь.
– Отойди, ты заслоняешь мне солнце, –
сказал Диоген и продолжал греться.
Исторический анекдот, известный по трудам Плутарха и Диогена Лаэртского

В начале 20-го века роль науки во всех сегментах культурной жизни и экономики оказалась настолько существенной, что потребовала осмысления самого этого явления. В рамках размышлений о науке философы рассматривали самые разные вопросы. Бертран Рассел в работе «Наука и религия» выдвинул тогда свой тезис об отсутствии этического вектора в науке и в научно-техническом прогрессе: наука не может быть ни добром, ни злом, это всего лишь техника, развитие греческого понятия «тэхне», инструментария жизни. Инструменты не имеют этического вектора: топором можно построить дом или убить соседа. Развитие технологий не меняет сути дела: микроскоп тоже не может быть ни добром, ни злом, он может послужить для создания и нового смертоносного вируса, и лекарства. Исследования атомного распада и ядерного синтеза породили как термоядерную бомбу, так и атомную энергетику…

На протяжении жизни нескольких поколений инженеров и ученых этический дискурс отсутствовал в сообществе естественных наук, он был исключен из профессионального мира, и это казалось вполне естественным. Ученые и инженеры редко задумывались о проблеме добра и зла в своей профессии. Областью их деятельности и творчества были техника, математика, фундаментальные и прикладные научные дисциплины. Научно-технический прогресс шел иногда равномерно, иногда скачкообразно, через научно-технические революции, но приверженность идеям Бертрана Рассела оставалась неизменной.

Computer Science и вопросы этики

Все изменилось 10–15 лет назад, когда одна из ведущих отраслей научно-технического прогресса – computer science (это можно перевести как «наука о компьютерах», в современном научном мире России такой дисциплины нет) – внезапно столкнулась с этическими проблемами и необходимостью для инженерного сообщества постоянного этического выбора. Случилось это в период разработки технологии Web 2.0 и систем саморазвивающегося контента. В рамках развития этой технологии возникло новое измерение в современных ИТ-системах – социальная инженерия профессиональных сообществ. Web 2.0 предусматривал «соработничество», сотрудничество различных специалистов, профессионалов и непрофессионалов, в разработке некоторого проекта. Например, профессионалы могут сформировать среду социальных сетей, но наполнение ее постами, фотографиями, другими материалами – это задача широких масс, которые бесплатно работают на проект.

С определенной точки зрения технология Web 2.0 сформировала идею эксплуатации в постиндустриальной и неклассовой экономике. Вовлекая в свои проекты множество людей, которые бесплатно отдавали свое личное время и свой труд на развитие коммерческих проектов, социальная инженерия современных ИТ создала идеальную модель эксплуатации: использо-

вание бесплатного труда наиболее креативной части населения в интересах обогащения новых капиталистов-технократов.

Как только в технические системы вошли элементы социальной инженерии, эти системы перестали быть сугубо технологическим явлением. Современные ИТ = технологии + компьютеры + люди, и коль скоро люди, коллективы, социальные группы стали частью технологии, в такой симбиоз неизбежно вернулись этический вектор и гуманитарное измерение. Человек является носителем своей этики, а также этических установок своего социума: профессионального сообщества, группы, народа, современной ему культуры. Его вовлеченность в современные компьютерные технологии привносит этический вектор и в них.

Социальная инженерия и технологии за последние десять лет причудливо переплелись. Можно говорить о явлении конвергенции – сплава технологий, которые уже не отделить друг от друга. Технологии computer science делают возможным развитие социальной инженерии вплоть до изменения смыслов, информации и восприятия человека. В то же время собранные и перепрограммированные социальной инженерией профессиональные группы целенаправленно развивают технологии computer science. Сейчас невозможно понять, где пролегает граница между одним и другим, – все сплавилось в единую систему, формируя уникальное явление – технико-гуманитарный дискурс. Современный специалист в области computer science с необходимостью должен быть универсалом в духе философов Возрождения, одновременно инженером и художником, ученым-естественником и философом-гуманитарием.

Но технико-гуманитарный дискурс несет в себе заряд этики. Все, что связано с человеком, неизбежно приводит к этическому выбору. Этический вектор оказался одним из элементов современных компьютерных технологий, неизбежным и неотвратимым. Каждый инженер, каждый аналитик в своей работе сталкивается с этическим выбором, время от времени или постоянно.

Что есть добро и зло

В этическом выборе computer science уже сейчас наметились определенные смыслы:

- все, что ведет к развитию, оптимизации и улучшению традиционных форм хозяйствования, может считаться добром;
- все, что предполагает радикальное преобразование самой природы человека либо общественных отношений или призвано свести положение человека к функции и механизму, явно относится к злу.

Как обычно, грань между добром и злом размыта, и в «пограничной зоне» возникают многочисленные споры. Сам факт таких споров – доказательство того, что традиционные ИТ вышли за границы чисто технического диалога о методах.

Споры вокруг «восстания машин», искусственного интеллекта, систем слежения за населением – все это споры этического плана. В последнее время, в особенности в связи с карантинными мероприятиями, все более популярен становится термин «электронный концлагерь» – как совокупный символ направления зла в технологии computer science. Алармизм нашего времени заключается в том, что символ добра в дискурсе отсутствует. «Цифровая экономика» пока слишком непонятна для того, чтобы стать символом оптимизации, а заимствованные термины – коллаборация, синергия, конвергенция и пр. – еще менее понятны. В отсутствие положительного символа возникает ощущение, что computer science – это только зло, что едва ли верно.

Новый план ГОЭЛРО

Современные компьютерные технологии могут решить историческую задачу социализма, построив идеальный Госплан. Можно рассуждать о том, что советская система экономики просто не дожила до современных компьютеров, а иначе победа СССР в экономической (холодной) войне была бы неизбежной. «Электронный Госплан», или iGOELRO может стать положительным символом возрождения экономики нашей страны, как в свое время план ГОЭЛРО стал символом индустриализации молодого советского – аграрного на тот момент – государства. Ведь и тогда дело было вовсе не в электрификации и электричестве. Но через электрификацию общество сделало свой этический выбор: достаточно вспомнить ленинскую формулу «Социализм – это советская власть плюс электрификация всей страны». В тот момент, на волне индустриальной революции, роли были четко разделены: технократы отвечали только за технологию и индустрию, политики – за смыслы и этику. В наше время computer science – это смесь того и другого.

Наше профессиональное сообщество пока не готово к этической дискуссии. Мы привыкли, что инженеры – вне политики, вне этики, мы работаем с технологиями и техникой. Но в современной жизни это уже не так. Этический вектор пришел к инженерам, и они с необходимостью должны стать политиками и гуманитариями.

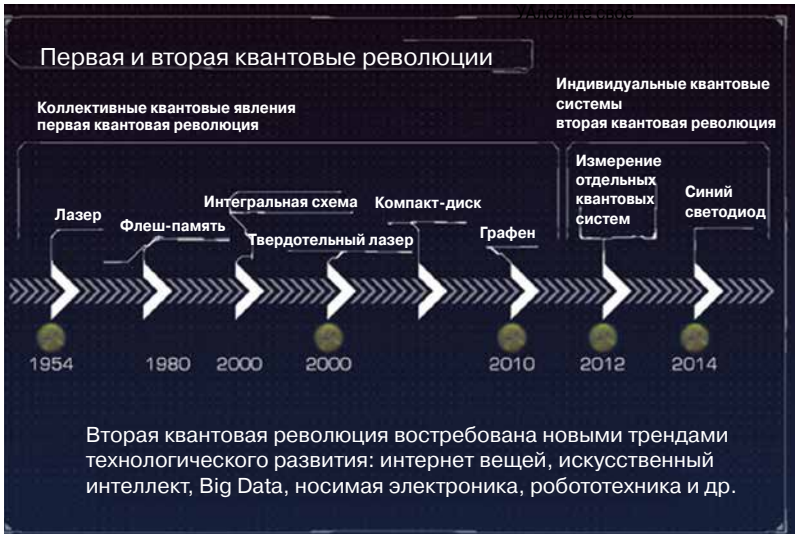
В этот непростой момент нужно четко понимать направления этического вектора: все, что ведет к «электронному концлагерю», – это зло, все проекты iGOELRO направлены на развитие и благоденствие нашей страны, и это – добро. Есть много пограничных областей, о них нужно говорить и спорить. Но если от нас требуется выбор, лучше понимать, между какими берегами странствует наш корабль... ИКС

Вторая квантовая революция: в погоне за лидерами

Николай Носов

На рубеже 21-го века мир оказался на пороге второй квантовой революции – способности управлять сложными квантовыми системами на уровне отдельных частиц, благодаря чему стало возможным создать системы квантового шифрования и вычислений.

В первой квантовой революции, начавшейся во второй половине 20-го века, технологии и приборы строились на управлении коллективными квантовыми явлениями (рис. 1). У человечества появились лазеры, транзисторы и компакт-диски. Без технологий первой квантовой революции было бы невозможно повсеместное распространение интернета и мобильной связи.



Источник: «Квантовый компьютер: большая игра на повышение». Лекция Алексея Федорова в Академии Яндекса

▲ Рис. 1. Первая и вторая квантовые революции

Квантовая случайность

Различные способы контроля над индивидуальными квантовыми объектами принято объединять термином «квантовые технологии». Пример применения квантовых технологий – генератор случайных чисел. Создание настоящей случайности – задача, трудно решаемая в макромире. Теоретически даже результат подбрасывания монетки можно рассчитать, если иметь все исходные данные. На практике используются псевдослучайные числа. Если какой-то умник поймет закономерность их генерации, то сможет взломать зашифрованные сообщения, подделать банковские платежные документы или разорить казино. В физике истинно случайной считается только квантовая случайность. Задача генератора случайных чисел – перенести ее из микромира в макромир.

Первый в мире квантовый генератор случайных чисел был создан женевской компанией ID Quantique. В ее разработке используется лазер с настолько низкой интенсивностью излучения, что в каждый момент времени существует только один квант электромагнитного излучения – фотон. Он попадает на полупрозрачное зеркало и случайным образом или проходит через него на детектор «1» или отражается на детектор «0». Детектор «1» генерирует единицы, детектор «0» – нули. Таким образом получается истинно случайная последовательность (рис. 2).

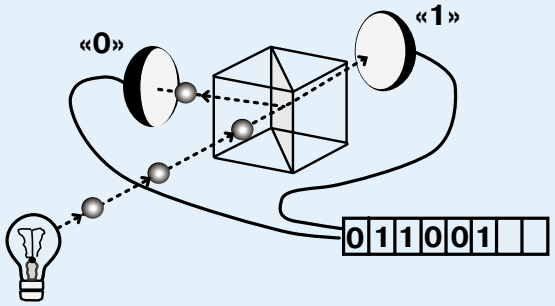
Бит и кубит

Существование истинной квантовой случайности, основы современных квантовых технологий, не всегда признавалось физиками. «Бог не играет со вселенной в кости», – сказал Нильсу Бору Альберт Эйнштейн. На что получил ответ: «Не указывайте Богу, что делать». Современная наука на стороне Бора. Есть законы больших чисел, тренды, статистические закономерности, но все характеристики конкретной элементарной частицы, основы мироздания, вероятностны до момента измерения.

Классический компьютер соответствует жестко детерминированному миру. Значение бита определяется однозначно: ноль или единица. Но мир не детерминирован. В квантовых вычислениях мир вероятностен. Аналог бита – кубит – описывается вероятностью нахождения в том или ином состоянии (рис. 3). Если бит можно уподобить лежащей на столе монетке с однозначно определяемым состоянием – орел или решка, то кубит – монетка, крутящаяся в воздухе или прыгающая в стакане, имеющая только вероятность оказаться в состоянии орел или решка. Говоря научным языком – система, находящаяся до измерения в состоянии суперпозиции.

Квантовая запутанность и квантовое шифрование

Квантовые объекты не являются ни классическими волнами, ни классическими частицами,



Источник: ID Quantique

◀ Рис. 2. Принцип работы квантового генератора случайных чисел, реализованный в ID Quantique

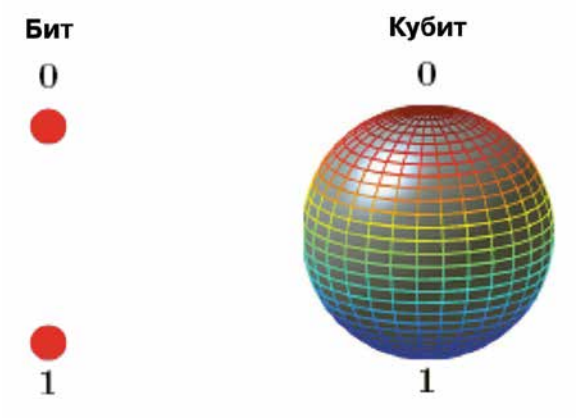


Рис. 3. ► **Кубит описывается вероятностью нахождения в одном из состояний («0» или «1»)**

проявляя свойства первых или вторых в зависимости от условий экспериментов, которые над ними проводятся. Причем в соответствии с принципом неопределенности Гейзенбе́рга, чем точнее измеряется одна характеристика объекта (энергия, спин, длина волны), тем менее точно можно измерить вторую. Квантовые объекты имеют неопределимые, вероятностные физические характеристики, которые хорошо подходят для использования в качестве кубитов – систем, находящихся в состоянии суперпозиции.

Однако мало иметь записанную в битах или кубитах информацию. Надо уметь ее передавать и обрабатывать. Ключевой феномен, используемый для обеспечения безопасности квантовой связи, – запутанность, т.е. взаимозависимость квантовых состояний двух или большего числа объектов.

Например, если послать зеленый фотон с определенной энергией на нелинейный кристалл, то из него вылетят два запутанных красных фотона. Определить энергию каждого нельзя, но если провести измерение энергии одного фотона, то, в соответствии с законом сохранения энергии, будет однозначно определена энергия второго, так как сумма энергий красных фотонов равна энергии зеленого.

Возраст (время до поимки детектором) красного фотона тоже до измерения не известен. Но он равен возрасту второго красного фотона, иначе был бы нарушен закон сохранения. Таким образом, между фотонами появляются квантовые корреляции. И если мы определим возраст одного фотона, то однозначно определим и возраст другого, который может находиться от первого на большом расстоянии.

Проведенные учеными эксперименты статистически опровергают естественное предположение о том, что динамические свойства квантовой частицы, наблюдаемые при измерении, реально существуют еще до измерения, а измерение лишь ликвидирует наше незнание того, какое именно свойство имеет место. На невозможности сохранения запутанности при попытке измерения параметров частицы третьей стороной построена невзламываемость квантовой связи.

Две стороны, соединенные по открытому каналу связи, могут создать общий случайный ключ, который известен только им, и использовать его для шифрования/дешифрования передаваемых пакетов информации. Если ключ попытается получить третья сторона, то она должна будет измерить передаваемые по каналу связи квантовые состояния, что приведет к их изменению и появлению аномалий, которые выдадут ее присутствие. Если количество аномалий ниже определенного порога, то ключ создается и безопасность передачи гарантируется, в противном случае секретный ключ не создается и связь прекращается.

Описанный выше метод квантового распределения ключей позволяет организовать полностью защищенные каналы связи, причем уже не только в лабораторных условиях. Впервые квантовое шифрование использовалось в 2007 г. для связи при проведении выборов в Федеральное собрание Швейцарии, затем в 2010 г. во время чемпионата мира по футболу в ЮАР.

В августе 2016 г. с космодрома Цзюцюань китайцы запустили первый в мире квантовый спутник «Мо-Цзы» (рис. 4). Аппарат обеспечил распределение запутанных фотонов на рекор-

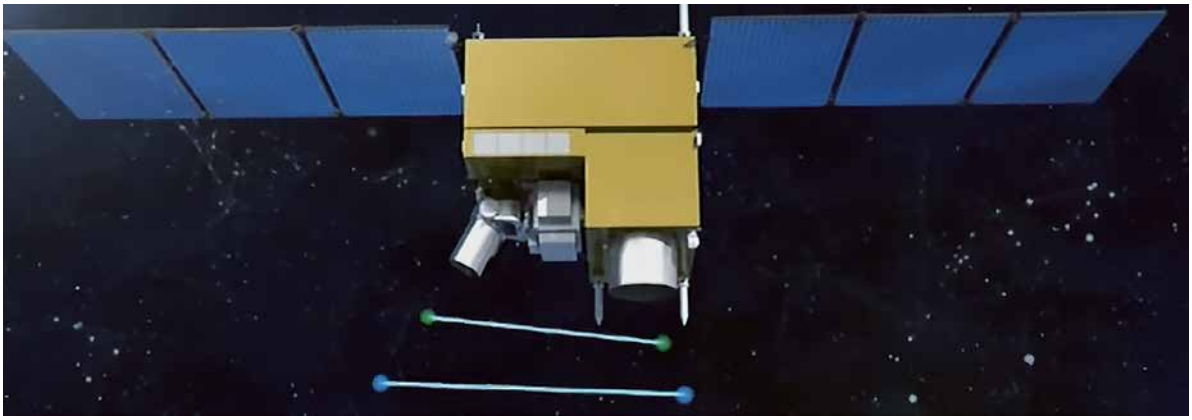


Рис. 4. ► **Квантовый спутник «Мо-Цзы», испускающий пары запутанных фотонов**

Источник: Asia Today

дно большое расстояние, свыше 1200 км. На космическом аппарате установили яркий источник запутанных фотонов – кристалл, в котором происходило спонтанное параметрическое рассеяние, т.е. превращение одного фотона в два с уменьшенной энергией. Источник формировал около 6 млн пар запутанных фотонов в секунду. Фотонные пары отправляли с помощью двух телескопов к наземным обсерваториям: Дэлинха (Тибет), Наньшань (Урумчи) и Гаомеигу (Юньнань). Как телескопы спутника, так и телескопы-приемники требовали высокой точности наведения – «Мо-Цзы» двигался по орбите со скоростью около 8 км/с.

В январе 2018 г. спутник «Мо-Цзы» передал реальные данные по защищенному каналу, связав австрийский Грац и китайский Синлун, расстояние между которыми составляет 7,6 тыс. км. Из Китая в Австрию отправили изображение древнекитайского философа, имя которого носит спутник, а в обратном направлении послали фото Эрвина Шредингера.

В марте 2019 г. в Британии была запущена первая в мире коммерческая квантовая сеть. Канал с квантовой защитой напрямую соединяет высокотехнологичные промышленные кластеры – Кембриджский научный парк и кластер Innovation Martlesham возле Ипсвича.

В январе 2020 г. появилось сообщение о создании в Китае первой в мире мобильной квантовой станции, подключаемой к спутнику «Мо-Цзы». Масса мобильного устройства квантовой связи составляет 80 кг. В кармане не унесешь, но уже можно установить на крыше автомобиля. Портативная станция в первую очередь разработана для китайских банков, которые уже используют спутниковую квантовую криптографию для связи отделений в разных частях страны. В ближайшие несколько лет ученые планируют запустить на орбиту небольшие спутники квантовой связи, целью которых будет обслуживание коммерческих клиентов.

Продолжаются эксперименты и с оптоволокном. Китайские специалисты использовали технологию квантовой связи при организации защищенного канала между Пекином и Шанхаем. В этой магистрали используются также традиционные сетевые компоненты, что создает риск взлома. А вот проект Делфтского технического университета предусматривает создание первой в мире сети, передающей информацию с помощью квантовых технологий из конца в конец, что можно считать прообразом невзламываемого интернета будущего. Строительство объединяющей четыре города голландской квантовой сети планируется завершить в 2020 г.

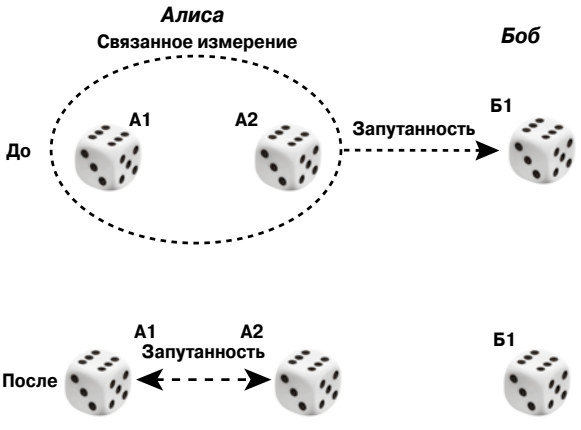
Квантовая телепортация

Квантовую связь можно использовать для квантовой телепортации, феномена, заключающегося в том, что вещество (масса, энергия) исходного объекта остается в точке отправления, но вся его структура (физическое состояние) просто исчезает. К примеру, если телепортируется пластилиновая утка, то пластилин остается на месте, но перестает иметь форму утки, делается бесформенным. А в пункте назначения бесформенная кучка пластилина (вещества) в конце процесса телепортации приобретет в точности форму исходной утки, вплоть до расположения отдельных атомов.

К сожалению, в макромире такое пока невозможно. А вот в микромире телепортация уже проводится, например, для фотонов. Фотон – пакет электромагнитной энергии, имеющий слабое колеблющееся электрическое поле. Если фотон имеет четкую поляризацию, электрическое поле регулярно колеблется в одном и том же направлении. Если фотон неполяризован, его колебания беспорядочны.

Принцип работы квантовой телепортации (рис. 5) таков: на стороне источника (Алиса) есть поляризованный фотон А1, по сути – квантовый кубит, который надо телепортировать. На стороне приемника (Боб) есть неполяризованный фотон Б1. У Алисы есть также фотон А2, запутанный с фотоном Б1. В процессе квантовой телепортации Алиса проводит связное измерение (запутывает фотон А1 с А2), в результате чего разрушается запутанность А2 и Б1, фотон А1 становится неполяризованным, а Б1 приобретает четкую поляризацию телепортированного фотона. Таким образом, фотон Боба становится во всем идентичен исходному фотону Алисы, а фотон Алисы А1 – исходному фотону Боба. Это и означает, что произошла телепортация квантового кубита.

Если у Боба есть фотон Б2, запутанный с фотоном Вики (В1), то при проведении Бобом связного измерения Б1 и Б2 образуется запутанность на



◀ Рис. 5. Принцип действия квантовой телепортации

Источник: Н. Жизан. «Квантовая случайность. Нелокальность, телепортация и другие квантовые чудеса»

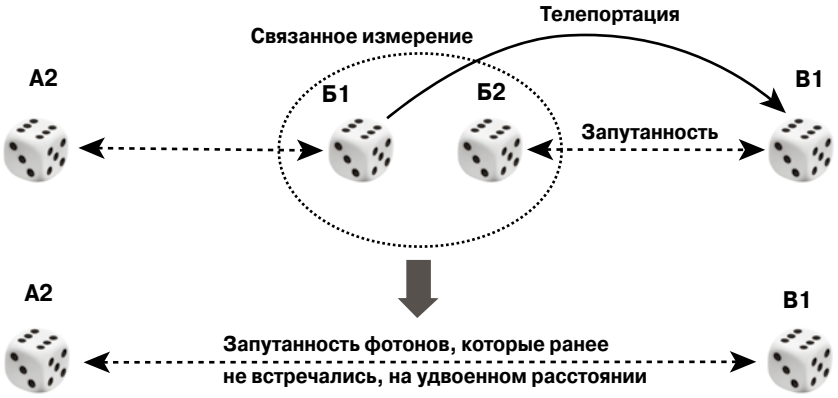


Рис. 6. ▶
Передача запутанности на расстояние

Источник: Н. Жизан. «Квантовая случайность. Нелокальность, телепортация и другие квантовые чудеса»

ность общения на уровне целой телепортационной сети, даже если между ними есть промежуточные узлы (квантовые повторители, как называют их физики).

В теории все выглядит убедительно, но на практике все совсем не просто. В настоящее время нет чисто однофотонных источников – в действующих установках используются слабые лазерные импульсы, где иногда проскакивают несколько фотонов, что дает возможность организовать атаку на канал связи. Кроме того, есть уязвимости у конкретных реализаций, что позволяет взломать квантовую систему, например, через насыщение принимающего фотодетектора.

еще большем расстоянии, причем между никогда не встречавшимися фотонами A2 и B1, и появляется возможность телепортировать A1 в B1 и далее (рис. 6). Передается форма, а не материя, так что фундаментальный закон, ограничивающий перемещение скоростью света, не нарушается.

Получившийся в итоге кубит не только находится в состоянии исходного кубита, но и абсолютно идентичен ему во всех смыслах. Этого нельзя достичь в рамках обычной побитовой передачи, поскольку для описания состояния квантовой системы необходимо бесконечное количество информации, ведь квантовых состояний бесконечно много. При обычной битовой передаче можно передать только приближенное описание состояния – чем точнее описание, тем больше его объем.

Состояние телепортируемого кубита неизвестно никому, в том числе отправителю и получателю. А любая попытка считать состояние на этапе передачи приводит к потере запутанности и невозможности телепортации. Алиса и Вика могут гарантировать конфиденциаль-

Степан Снигирев, канд. физ.-мат. наук, экс-сотрудник Института квантовой оптики общества Макса Планка (Гархинг, Германия)

Пока все решения нишевые. Квантовая связь позволяет соединить через спутник или оптоволокно только две точки. Причем на обоих концах используется дорогое оборудование. Отсутствие асимметричного квантового шифрования требует интерактивного взаимодействия – если принимающая сторона находится в офлайне, то через канал квантовой связи послать сообщение нельзя. До невзламываемого интернета с возможностью защищенной связи с несколькими точками очень далеко. В ближайшее время технология вряд ли дойдет до широкого потребительского рынка.

Квантовая связь в России

До телепортации в макромире еще далеко, да и неизвестно, осуществима ли она в принципе. А вот квантовые коммуникации вполне возможны. В том числе в России, где отставание от лидирующих области квантовых технологий США, ЕС и Китая быстро сокращается.

В июне 2016 г. сотрудники «Российского квантового центра» (РКЦ) соединили квантовой связью два здания Газпромбанка в Москве. В мае 2017 г. специалистам РКЦ удалось создать многоузловую гетерогенную квантовую сеть передачи данных. Ученые смогли применить одновременно два метода шифрования данных в одной сети. На одном участке сети информация шифровалась путем поляризации фотонов (этот метод разработан в РКЦ), во втором задействовалась их фаза.

В конце 2019 г. «Ростелеком» начал работы над проектом «Ландау» создания защищенной квантовой линии связи между своими датацентрами в Москве и в Удомле (Тверская область). Первую в России коммерческую линию квантовой связи длиной 670 км построят в 2021 г., к концу 2020-го должен появиться прототип данного сервиса. В качестве канала связи используют оптоволокно. Проблему рассеивания фотонов в оптоволокне разработчики «Ростелекома» планируют решить, построив на линии шесть защищенных промежуточных узлов. В перспективе квантовую сеть намереваются продлить до Санкт-Петербурга.

Мало передать запутанные фотоны – нужно иметь оборудование для их использования. В этом направлении тоже ведутся работы. Компания «Инфотекс» создала комплекс аппаратуры, включающий подсистему квантового распределения ключей и два скоростных шифрато-

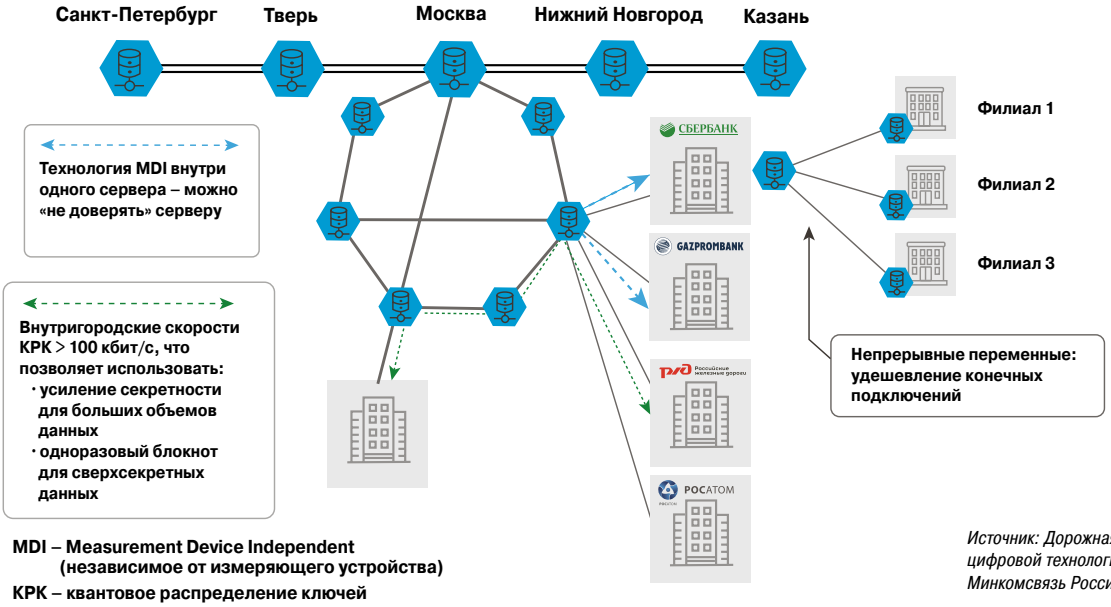
ра. ViPNet Quandor стабильно вырабатывает секретный квантовый ключ длиной 256 бит в среднем 1 раз в минуту. Это позволяет шифровать большой объем пользовательского трафика на высокой скорости. Весной 2019 г. компания «Инфотекс» и Центр квантовых технологий МГУ представили первый в России телефон с квантовой защитой связи ViPNet QSS Phone (рис. 7). Устройство шифрует голосовой трафик между стационарными IP-телефонами с помощью квантового распределения ключей.

◀ Рис. 7.
Квантовый телефон ViPNet QSS Phone

Источник: «Инфотекс»

В июле 2019 г. после подписания соглашения о намерениях между РЖД и правительством России появилось сообщение о планах компании создать квантовую сеть для безопасной передачи данных. РЖД намеревается вложить в развитие квантовых технологий в нашей стране 24,7 млрд руб. Согласно проекту «дорожной карты», часть средств будет потрачена на квантовую сеть для 1000 абонентов, которая будет построена к 2024 г. Развертыванием квантовых сетей в РЖД займется специально созданный департамент квантовых коммуникаций.

Над квантовыми сетями в России работают и другие компании. Так, компания СМАРТС получила грант Российского фонда развития информационных технологий на строительство магистральной квантовой сети от Самары до Сызрани. Строительство планируется завершить до конца 2020 г.



◀ Рис. 8.
Инфраструктура квантовых сетей в РФ к 2024 г.

Источник: Дорожная карта развития «сквозной» цифровой технологии «Квантовые технологии», Минкомсвязь России

В октябре 2019 г. Минкомсвязь России опубликовала документ «Дорожная карта развития “сквозной” цифровой технологии “Квантовые технологии”», разработанный в рамках направления «Цифровые технологии» нацпрограммы «Цифровая экономика РФ». В документе квантовая связь называется наиболее зрелой и близкой к массовому внедрению квантовой технологией и приводится пример инфраструктуры квантовых сетей в РФ к 2024 г. (рис. 8). На схеме показаны уже строящиеся каналы квантовой связи (Москва – Тверь) и возможные в ближайшем будущем продолжения (Тверь – Санкт-Петербург, Москва – Нижний Новгород – Казань).

В дорожной карте отмечается, что «новые решения должны позволить перейти от решений "точка–точка" к архитектуре "звезда" со снижением стоимости подключения и к решениям без требования к доверию промежуточному узлу».

Поздний старт привел к тому, что в 2016 г. Россия отставала от лидеров на 10–12 лет, но это отставание сокращается, в 2019 г. оно оценивалось уже в три-четыре года. На государственном уровне ставится задача к 2024 г. отставание ликвидировать и занять 8% мирового рынка квантовых коммуникаций. Среди приоритетных направлений использования – защита национальных информационно-коммуникационных сетей, обеспечение защиты информации для финансового сектора, государственных органов, крупных технологических компаний и держателей критической информационной инфраструктуры.

Квантовые вычисления: технологии и проблемы

Квантовые эффекты – суперпозицию и запутанность – можно использовать для квантовых вычислений: решения задач в области криптографии, машинного обучения и моделирования поведения квантовых систем.

Преимущества квантовых вычислений

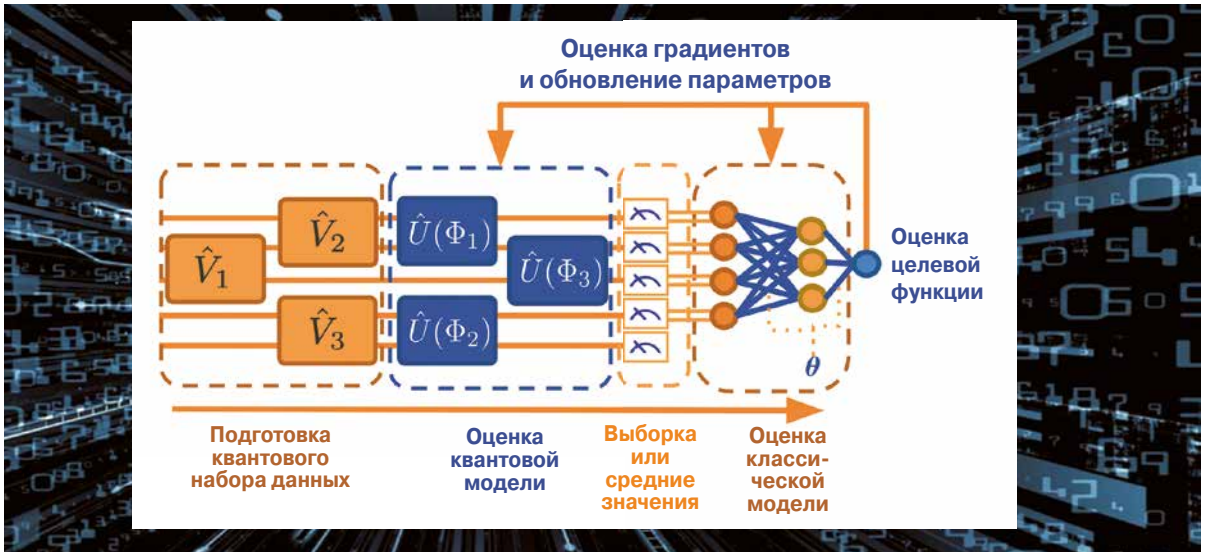
Многие задачи компьютер решает простым перебором вариантов. Например, трех человек по двум поездам можно рассадить восемью (2^3) способами – это легко решаемая задача. При увеличении размерности исходных данных пространство решений растет по степенному закону. Если людей будет 100, то вариантов решений – 2^{100}, и с задачей не справится самый мощный современный суперкомпьютер.

Квантовый компьютер оперирует кубитами – элементами, находящимися в состоянии квантовой суперпозиции. Каждому человеку в рассматриваемой задаче будет соответствовать кубит. Задача будет решаться вероятностным моделированием – многократным «подбрасыванием монет». Для получения результата надо много раз запустить квантовый алгоритм на одном и том же наборе входных данных и усреднить результат. Время выполнения квантового алгоритма можно считать постоянным (с некоторыми допущениями) по отношению к размерности пространства решений (2^N). И чем выше размерность, тем больше преимущество во времени выполнения вычислений у квантовых компьютеров по сравнению с классическими.

Задачи перебора – основной тип задач, ускоряемых квантовыми алгоритмами. Устройства, производящие квантовые вычисления, могут многократно превосходить классические компьютеры при решении задач криптоанализа, моделирования сложных систем, а также машинного обучения и искусственного интеллекта.

Например, полный перебор вариантов (brute force) – наиболее универсальный метод криптографической атаки, т.е. подбора пароля или ключа шифрования. Он также может задействоваться для поиска оптимальных параметров в любом множестве, что используется в задачах машинного обучения и ИИ. Метод можно применять вместо или в комбинации с различными аналитическими алгоритмами, сокращающими объем вычислений в процессе поиска экстремумов целевых функций.

Гибридный подход продвигает Google. В марте 2020 г. компания анонсировала работающую на классических компьютерах систему машинного обучения TensorFlow Quantum, «понимающую» квантовый язык программирования Cirq. Здесь на вход нейронной сети поступает выборка (средние значения) данных (см. рисунок), полученная в квантовой модели. Гибридная квантово-классическая конфигурация позволяет ускорить процесс обучения нейронных сетей.



Гибридная квантово-классическая нейронная сеть, использующая TensorFlow Quantum ▶

Источник: Google

Машинное обучение – одна из сфер, развитию которых квантовые вычисления могут дать дополнительный импульс. Речь идет о широкой исследовательской программе. Нужно изучить, как квантовые компьютеры могут ускорить отдельные элементы алгоритмов машинного обучения (например, решение систем линейных уравнений) и насколько они могут быть полезны для оптимизации. Исследуется ускорение обучения нейронных сетей определенного класса с использованием квантовых и квантово-вдохновленных алгоритмов (классических алгоритмов, которые моделируют поведение квантовых систем).

Сложности практики

В теории квантовые вычисления выглядят многообещающе, но реализовать их на практике весьма и весьма непросто.

Прежде всего, кубиты крайне нестабильны – даже незначительные внешние воздействия нарушают запутанность. Чтобы избежать этого, используют камеры с максимальной изоляцией от воздействий внешней среды и температурой внутри чуть выше абсолютного нуля. И все равно максимальное время жизни квантовой системы, когда она пригодна для квантовых вычислений (время декогеренции), крайне мало. По данным ресурса Quantum Computing Report, сейчас время декогеренции не превышает сотен микросекунд, рекорд – 148,5 мкс – принадлежит 20-кубитовому компьютеру IBM в Токио. Через указанное время система начнет выдавать белый шум вместо вероятностных распределений. А за этот короткий период надо инициализировать систему кубитов, провести вычисления и получить результат.

Другое препятствие при выполнении на квантовых компьютерах сложных, длинных алгоритмов – наличие ошибок. Вероятность возникновения ошибок при вычислениях, считывании и записи информации возрастает вместе с ростом количества кубитов. Стандартные методы коррекции ошибок (дублирование вычислений и усреднение) в квантовом мире не работают. Приходится прибегать к специальным квантовым методам коррекции ошибок, когда из нескольких обычных кубитов формируется один логический кубит. «Если каждый физический кубит будет работать с одним логическим, то каждая операция будет разрушать состояние запутанности и можно будет провести лишь малое количество операций. В качестве альтернативы можно объединить десять кубитов в кластер и использовать их как один логический кубит. Количество операций, выполняемых с такими логическими кубитами, можно увеличить на два порядка. То есть на порядок уменьшаем число кубитов, но на два порядка увеличиваем число операций, которые с ними можно проводить», – поясняет экс-сотрудник Института квантовой оптики общества Макса Планка канд. физ.-мат. наук Степан Снигирев.

> Квантовые вычисления сдвигают границу между построенной на расчетах физикой и химией, где ответ может дать только эксперимент. Например, все необходимые уравнения для нахождения волновой функции атома лития давно известны, но даже для такого простого атома моделирование на классическом компьютере является сверхсложной задачей. Квантовые компьютеры могут решать уравнения Шрёдингера экспоненциально быстрее классических и больше подходят для моделирования физических систем на микроуровне (задач Фейнмана).

Алексей Федоров, руководитель научной группы «Квантовые информационные технологии» Российского квантового центра

Для решения практических задач нужно радикально увеличить число используемых кубитов. Наращивание числа кубитов в квантовом компьютере – сложный технологический процесс. В лучших универсальных, предназначенных для решения широкого круга задач квантовых компьютерах их сейчас не более сотни (см. таблицу).

Кубит можно запутать только с соседними. Но даже в лучших по этому параметру квантовых компьютерах IBM удается запутать только шесть соседних кубитов. Для того чтобы запутать более дальние, приходится строить цепочку дополнительных квантовых операций, использовать дополнительные кубиты и, соответственно, увеличивать общий уровень ошибок.

Максимальное число кубитов, запутанность и время декогеренции ▼

Компьютер	Число кубитов	Число запутанных кубитов			Время декогеренции, мкс		
		Мин.	Макс.	Средн.	Мин.	Макс.	Средн.
Google Sycamore	53	1	4	3,25	9,7	27,8	16,04
IBM Rochester	53	1	3	2,15	TBD	TBD	TBD
IBM Q20 Austin	20	2	6	3,9	N/A	N/A	102,6

TBD – будет объявлено дополнительно; N/A – нет данных

Источник: Quantum Computing Report, апрель 2020

В борьбе за кубит

Разработчики стремятся создать компьютеры, которые могли бы контролировать больше кубитов, для более длинных вычислений и с меньшим количеством ошибок. При этом используются разнообразные технологии, обеспечивающие суперпозицию и запутанность кубитов.

В кубитовой гонке лидируют технологии сверхпроводящих кубитов. По сути это микросхемы из сверхпроводника со специальными элементами – джозефсоновскими переходами, представляющими собой наноразмерные разрывы в сверхпроводнике. Сверхпроводящий ток, циркулирующий в таких микросхемах, ведет себя как один большой квантовый объект и обладает ровно двумя необходимыми базисными состояниями, определяемыми либо направлением тока – по часовой стрелке или против, либо количеством носителей заряда (пар электронов) на отдельных элементах микросхем.

Сверхпроводящие кубиты можно произвольным образом размещать на чипах и изготавливать с помощью зрелых технологий производства полупроводниковой промышленности. Управлять ими проще, чем многочисленными атомами или ионами. На них делают ставку гиганты индустрии IBM, Google и Rigetti, создающие кубиты на кремниевых чипах, которые охлаждают почти до абсолютного нуля.

В качестве кубитов можно использовать захваченные ионы, внутренними уровнями энергии которых можно управлять с помощью лазера. Кубиты в новых квантовых системах стартапа IonQ представляют собой отдельные атомы редкоземельного элемента иттербия, взвешенные в вакууме. Информация хранится, обрабатывается и извлекается из атомов с помощью точно направленных лазерных лучей. Этот подход, называемый захватом ионов, теоретически эффективен, но технически сложен – работать с такими системами можно только в установках с ультравысоким вакуумом, предварительно охладив частицы до тысячных долей градуса выше абсолютного нуля с помощью лазерного охлаждения.

Теоретически кубитами для квантового компьютера могут служить и фотоны в волноводах. Реализовать вычислительные алгоритмы с помощью таких кубитов можно, но при масштабировании системы возникают серьезные проблемы, и предпочтительным направлением для использования кубитов на фотонах считаются квантовые коммуникации.

Изучается возможность задействовать кубиты, основанные на явлении ядерного магнитного резонанса (ЯМР): для кодирования состояния служат спины атомных ядер во внешнем магнитном поле. При таком подходе логические операции совершаются не над отдельными спинами, а над совокупностью всех молекул в используемом веществе (в первых экспериментах – жидкости). Количество взаимодействующих друг с другом молекул в рабочем объеме вещества достигает нескольких триллионов. Несмотря на то что были созданы 12-кубитовые квантовые процессоры и продемонстрирована возможность запускать на них квантовые алгоритмы, дальнейшее развитие вызывает у специалистов сомнения из-за сложностей управления столь большим числом квантовых состояний.

Эволюцией жидкостных ЯМР-кубитов можно считать кубиты на твердотельных дефектах в кристаллах. Такие дефекты могут быть изготовлены с помощью облучения в нужных местах бездефектного материала пучком заряженных частиц. Особая электронная структура этих дефектов позволяет им реагировать на облучение лазерным лучом и испускать флуоресцентное излучение с большей по сравнению со светом лазера длиной волны. При этом состояние электронов в дефекте может быть использовано в качестве базисных состояний кубитов. Наиболее пригодны для квантовых вычислений азотные дефекты в алмазах, а также фосфорные дефекты в кремнии.

Дефект не нужно удерживать внешними электромагнитными полями, как в случае ионов, и охлаждать до низких температур, что открывает перспективы для коммерческих решений. Впрочем, масштабировать подобные решения также очень сложно.

В 2019 г. группа немецких физиков под руководством Герхарда Биркла, используя созданный с помощью оптической ловушки бозе-конденсат холодных атомов, смогла получить систему из 111 атомов рубидия, пойманных в оптическую ловушку. Каждый атом в этой системе соответствует одному кубиту, а спин атома определяет его состояние: если спин смотрит вверх, в кубит записана единица, в противном случае – ноль. Технология холодных атомов выглядит обещающе в плане дальнейшего масштабирования, особенно если удастся решить проблему дефектов решетки, в которой «сидят» атомы, – в каждом узле должен находиться только один атом.

Корпорация Microsoft изучает возможность применения кубитов на майорановских фермионах. Преимущество технологии – возможность сохранения квантового состояния в течение длительного времени. Теоретические работы подтверждают возможность масштабирования таких систем до полноценного квантового компьютера, но пока на таких кубитах еще не удалось продемонстрировать логические операции, не говоря уже о квантовых алгоритмах.

Один из наиболее экзотических вариантов построения кубитов – использование поляритонов, квазичастиц, которые являются наполовину светом (фотоном), наполовину материей (атомом). В момент столкновения фотонов с охлажденными почти до абсолютного нуля атомами рубидия фотоны приобретают массу (атомная составляющая поляритона). Путешествуя через облако рубидия, фотоны движутся от атома к атому. Иногда происходят встречи фотонов, после которых они следуют вместе неразрывно. Покинув облако, они теряют атомную составляющую, но «помнят» о том, что происходило с ними в облаке, оставаясь связанными в пары и триплеты, что может найти применение в квантовых вычислениях.

Способов запутывания квантовых кубитов много, и здесь перечислены далеко не все платформы построения квантового компьютера. Какая технология наиболее перспективна? Это один из наиболее важных вопросов в области квантовых вычислений. Ответ на него неизвестен. Сверхпроводящие цепочки, нейтральные атомы, ионы в ловушках, оптические системы активно развиваются, конкурируют и демонстрируют схожие показатели по количеству кубитов и качеству работы с ними. «На мой взгляд, для каждой из платформ могут быть найдены интересные приложения. Ярко выраженный лидер может появиться на горизонте трех–семи лет. Это будет система, с помощью которой можно будет решать практические задачи», – считает Алексей Федоров, руководитель научной группы «Квантовые информационные технологии» Российского квантового центра.

На пороге посткремния

В области квантовых вычислений за последние годы удалось достичь значительного прогресса. Но до практического их использования далеко даже лидерам гонки.

В опубликованном в 2019 г. журналом Массачусетского технологического института списке технологических прорывов прошедшего года к квантовым вычислениям относились сразу два пункта – невзламываемый интернет и достижение квантового превосходства, т.е. демонстрация квантовым компьютером вычислительной мощности, которую невозможно обеспечить при использовании самых современных классических компьютеров. Реальные возможности квантовой связи и невзламываемого интернета обсуждались в предыдущих статьях. Теперь попробуем разобраться с квантовыми вычислениями и их перспективами.

Квантовые алгоритмы

Процесс вычислений квантового компьютера можно представить как изменение начального состояния системы кубитов с помощью некоторых специальных преобразований, соответствующих логическим операциям. В конце измеряются характеристики системы – результат работы компьютера. Квантовая система дает результат, который можно считать правильным лишь с некоторой вероятностью. Но путем многократного повторения алгоритма (увеличения числа «подбрасываний монетки») вероятность правильного результата можно приблизить к единице.

В классическом компьютере используются логические вентили – базовые элементы цифровых схем, которые выполняют элементарные логические операции (побитовое отрицание, «И», «ИЛИ», «исключающее ИЛИ», побитовые сдвиги) и преобразуют входные логические сигналы в выходной. В квантовом компьютере вентили, соответственно, квантовые, преобразующие входные состояния кубитов в выходные по определенному закону. Простейшие однокубитовые вентили: тождественное преобразование, отрицание, фазовый сдвиг и др.

Обычные алгоритмы, основанные на бинарной логике, непригодны для квантовых компьютеров, использующих квантовую логику (квантовые вентили). Для них нужны специальные алгоритмы, задействующие квантовые преобразования. Разработка таких алгоритмов – сложная задача. Ее решением, не дожидаясь появления промышленных квантовых компьютеров, занимается ряд компаний, в том числе Google и Microsoft. Кроме того, проверка результатов вычислений квантового компьютера на классическом тоже представляет собой проблему. Для задач большой размерности это просто невозможно – не хватит вычислительных ресурсов самого мощного суперкомпьютера.

Не стоит забывать, что программы для квантовых компьютеров пишутся на классических компьютерах, эмулирующих работу квантовых. Разная архитектура квантовых процессоров приводит к тому, что первоначально программы пишутся для эмулятора «связность всех со всеми», а затем их приходится перекоm-

пилировать, чтобы они отвечали особенностям архитектуры конкретного процессора. Это еще больше усложняет процессы разработки.

Сегодня наиболее известны квантовые алгоритмы Шора (разложение чисел на простые множители), Гровера (решение задачи перебора) и Дойча – Йожи (ускорение перебора). Это работа на перспективу – когда кто-нибудь построит пригодный для промышленной эксплуатации универсальный квантовый компьютер, уже будет в наличии инструментарий для написания программ.

Специализированные квантовые компьютеры

Однако универсальный, т.е. решающий любые задачи, квантовый компьютер построить очень сложно. Чтобы решать реальные задачи, надо на несколько порядков увеличить количество кубитов квантового компьютера и количество операций, которые можно над ними производить. Быстрее можно добиться прогресса в аналоговых квантовых компьютерах – квантовых симуляторах, в которых при помощи одной хорошо контролируемой квантовой системы имитируется другая.

Квантовые симуляторы используются, в частности, для моделирования поведения твердых тел. Например, с помощью симулятора на холодных нейтральных атомах можно описать поведение электронов в кристаллической решетке. Симуляторы на холодных ионах помогут изучить колебания и деформации кристаллической решетки. Другие типы квантовых симуляторов – на наноалмазах с примесями, на сверхпроводящих цепочках и на ядерных спинах.

Широкую известность получили чипы компании D-Wave, которые уже применяют Google и NASA. В этих чипах используется эффект квантового туннелирования (преодоление микрочастицей потенциального барьера в случае, когда ее полная энергия меньше высоты барьера), который существенно повышает скорость работы алгоритма решения задач глобальной оптимизации. По сути это квантовый аналог интегральных схем специального назначения, предназначенный для одного алгоритма.

Рис. 1.
Квантовый компьютер IBM Q System One ▼

Источник: IBM

Лидеры квантовой гонки

В квантовые технологии вкладываются огромные средства. Конгрессом США утвержден проект развития квантовых технологий стоимостью $20 млрд, в Европе действует программа Quantum Flagship (после завершения предыдущей программы 2013–2016 гг.) с бюджетом более 3 млрд евро, в Китае создается Национальная квантовая лаборатория, в которую планируется инвестировать до $12 млрд.

Лидирующие позиции в квантовой гонке занимают американские компании. В 2001 г. IBM построила 7-кубитовый квантовый компьютер, использующий технологию ядерного магнитного резонанса, и успешно выполнила на нем алгоритм Шора. В ноябре 2009 г. физики Национального института стандартов и технологий США впервые собрали программируемый квантовый компьютер из двух кубитов. В феврале 2012-го IBM создала кремниевый чип на трех сверхпроводящих кубитах, а в апреле того же года ученые из ряда американских университетов построили двухкубитовый квантовый компьютер на кристалле алмаза с примесями, работающий при комнатной температуре. В ноябре 2017 г. IBM представила прототип процессора с 50 кубитами. В январе 2018 г. компания Intel анонсировала сверхпроводящую микросхему Tangle Lake с 49 кубитами. В марте Google объявила, что ей удалось построить 72-кубитовый квантовый процессор Bristlecone.

В прошлом году компания IBM представила на выставке CES 2019 в Лас Вегасе квантовый компьютер IBM Q System One (рис. 1), который позиционирует как первый коммерческий квантовый компьютер в мире. Событие важное, но 20 кубитов – очень мало для решения практических задач. Область применения компьютера крайне ограничена, и коммерческий успех вызывает большие сомнения.

Россия догоняет

Россия включилась в квантовую гонку с заметным отставанием. В мае 2015 г. ученые МФТИ, МИСиС и ИФТТ РАН создали первый отечественный кубит. Для этого были использованы два сверхпроводника, разделенные тонким слоем диэлектрика. В октябре 2017 г. сотрудники физического факультета МГУ им. М.В. Ломоносова представили установку, позволяющую из-

◀ Рис. 2.
Квантовые вычисления для решения задач индустрии к 2024 г.

Источник: Дорожная карта развития «сквозной» цифровой технологии «Квантовые технологии», Минкомсвязь России

готавливать компактные оптические элементы для чипов квантового компьютера.

В феврале 2018 г. был сформирован российский консорциум для создания многокубитового компьютера. Внешэкономбанк, «ВЭБ Инновации», Фонд перспективных исследований, МГУ и АНО «Цифровая экономика» подписали соглашение об осуществлении проекта создания отечественного многокубитового (не менее 50 кубитов) оптического квантового симулятора. В апреле 2018 г. был представлен проект техзадания на создание отечественного 50-кубитного квантового компьютера, который, в частности, определил основные требования к разработке оптического квантового симулятора на базе двух технологий – фотонных чипов и нейтральных атомов.

В 2019 г. госкорпорация «Росатом» запустила масштабный (бюджет – более 20 млрд руб.) проект создания отечественного квантового компьютера. В числе задач – объединение усилий в разработке квантового программного обеспечения и квантовых алгоритмов, поддержка всех центров компетенции и развитие различных платформ создания кубитов: сверхпроводников, фотонов, холодных атомов и ионов.

Упоминавшаяся в предыдущей статье «Дорожная карта развития “сквозной” цифровой технологии “Квантовые технологии”», разработанная Минкомсвязью России, предусматривает, что к 2024 г. число кубитов в сверхпроводниковом квантовом компьютере должно быть доведено до 30–50, до текущего уровня у лидирующих стран. То есть планируется сократить отставание от лидеров до четырех лет.

Как отмечается в дорожной карте, главным потребителем квантовых технологий является государство, что объясняется стратегической важностью квантовых технологий для обеспечения национальной безопасности. А основой для доступа к технологиям квантовых вычислений будет выступать облачная платформа (рис. 2).

Дорожная карта объединяет все ведущиеся работы в рамках единой логики: построение полного стека квантовых вычислений путем создания различных прототипов квантовых процессоров и обеспечения к ним облачного доступа. Для этого нужно будет разработать как «железо» (выбраны четыре платформы: сверхпроводники, атомы, ионы и фотоны), так и программное обеспечение (включая компиляторы и языки программирования). Если говорить о параметрах, то это системы из 30–100 кубитов в зависимости от реализации. «На мой взгляд, первые практические задачи будут связаны с квантовой химией и оптимизацией. По направлению квантовой химии уже выполняются прикладные исследовательские проекты, например, Российский квантовый центр

◀ Текущее состояние квантовых вычислений в России и целевые показатели развития до 2024 г.

Показатель	2019	2021	2024
Количество кубитов в сверхпроводниковом квантовом компьютере	2	5–10	30–50
Количество кубитов в квантовом компьютере на нейтральных атомах	10	50	100
Количество кубитов в квантовом компьютере на ионах	1	5	55

Источник: Дорожная карта развития «сквозной» цифровой технологии «Квантовые технологии», Минкомсвязь России

ведет такие исследования в интересах компании Nissan», – сообщил руководитель научной группы «Квантовые информационные технологии» Российского квантового центра Алексей Федоров.

Так ли превосходно квантовое превосходство?

Новые технологии добиваются успеха, когда демонстрируют свое превосходство над уже используемыми. Квантовый компьютер – когда достигнет квантового превосходства или хотя бы квантового преимущества, т.е. способности решать проблемы быстрее, чем классические компьютеры.

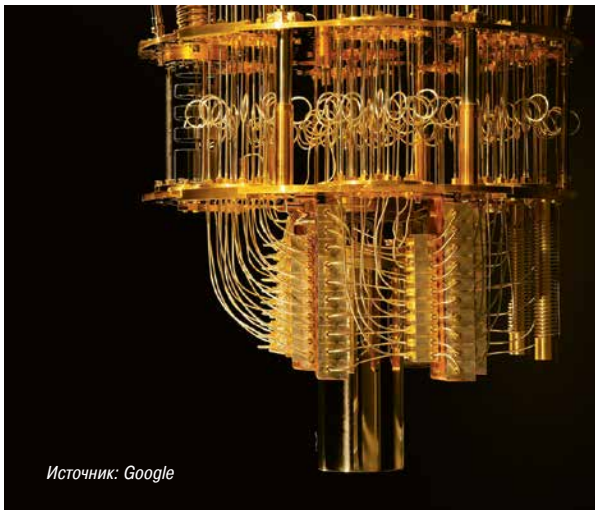
В октябре 2019 г. компания Google заявила о первой демонстрации «квантового превосходства». Компьютер Sycamore (рис. 3) с 54 кубитами, из которых 53 были функциональными и использовались для расчетов, чуть больше чем за три минуты выполнил объем вычислений, который, по оценке компании, занял бы у самого большого на сегодня суперкомпьютера в мире 10 тыс. лет. Это означает, что квантовый компьютер справился с задачей в 1,5 млрд раз быстрее.

С заявлением Google не согласилась компания IBM – при использовании классическим компьютером специальных алгоритмов решения представленной задачи выигрыш во времени будет измеряться только тысячами раз, поэтому речь идет не о квантовом превосходстве, а лишь о квантовом преимуществе. Но в любом случае достижение Google – крупная веха в развитии квантовых компьютеров.

Сергей Абрамов, директор, Институт программных систем им. А.К. Айламазяна РАН

Мы стоим на пороге эпохи посткремниевых вычислений, которые могут быть реализованы разными способами. Предлагаемые подходы, как правило, не универсальны, применимы не для всех классов задач и могут рассматриваться только как дополнение к классическим кремниевым вычислителям. Это справедливо и для наиболее распиаренных квантовых вычислителей, способных решать пока достаточно узкий класс задач.

Казалось бы, дело за малым – довести технологии до этапа промышленной эксплуатации. Однако сейчас все представленные решения узкоспециализированные или мало масштабируемые. Инженеры Google считают, что используемый ими подход может привести их к компьютеру со 100–1000 кубитами, чего может быть достаточно для практического применения.



▲ **Рис. 3. Квантовый компьютер Sycamore**

Для спецслужб привлекательной выглядит идея взлома чужих шифров. На решение такой задачи никаких денег не жалко. Однако угрозы современной криптографии со стороны квантовых компьютеров сильно преувеличены. С учетом используемых алгоритмов оптимизации для взламывания современных шифров потребуется порядка 100 тыс. кубитов и порядка миллиона производимых с ними операций. В настоящий момент – цифры совершенно нереальные. Да еще надо решить проблему ошибок. Пусть каждая квантовая операция имеет достоверность 99,9%. Но если надо выполнить тысячу таких операций, то вероятность ошибки станет огромной.

Потенциал современных кремниевых компьютерных технологий почти исчерпан. Уменьшать размеры компонентов электронных устройств дальше нельзя из-за квантовых эффектов – на таком уровне вещество проявляет волновые свойства, и начинает действовать принцип неопределенности Гейнзенберга. Однако квантовые вычисления не единственный, а один из возможных дальнейших путей развития. Есть проекты фотонных вычислителей, мемристоров и иных нейроморфных архитектур, биокомпьютеров, вычислителей, построенных на обратимых процессах и др. Но все они далеки от практического применения.

Развитие квантовых вычислений напоминает ситуацию с промышленным термоядерным синтезом, превратившемся в «вечно грядущую» технологию, которая всегда в разработке, всегда где-то там, в полувеке от нас. Однако квантовые (или неквантовые, но в любом случае посткремниевые) вычисления непременно станут нашим настоящим, причем, весьма вероятно, что в не слишком отдаленной перспективе. ИКС

DWDM «Волга» для ЦОДов

Владимир Трещиков, генеральный директор, «Т8»

Разработанные для дата-центров DCI-решения российской компании «Т8» радикально увеличивают скорость, снижают стоимость передачи данных и способствуют повышению информационной безопасности страны.

Объем данных, передаваемых по каналам связи дата-центров, стремительно растет. Прокладывать новые кабели, чтобы справиться с трафиком, – долго и дорого, а в крупных городах и не всегда возможно. Самый простой вариант нарастить пропускную способность уже действующего оптоволокна – установить оборудование плотного мультиплексирования с разделением по длине волны (Dense Wavelength Division Multiplexing, DWDM).

Разработкой таких устройств для магистральных, региональных и городских сетей, дата-центров и транспортных сетей 5G занимается российская компания «Т8», входящая в десятку мировых лидеров на рынке DWDM-систем. Передовые позиции – следствие высокой надежности изделий, подтвержденной опытом эксплуатации на магистральных сетях «Ростелекома».

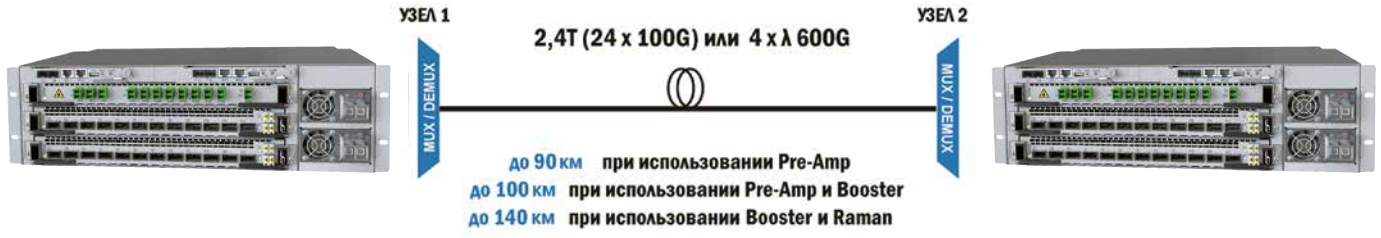
Новая компактная трехъюнитовая система «Волга» V3-DCI (COMPACT), разработанная «Т8», предназначена в первую очередь для соединений между ЦОДами. Достоинства модели – увеличенная втрое по сравнению с предыдущим поколением скорость передачи данных (до 600 Гбит/с на канал) и компактность, благодаря чему она занимает минимум места в дата-центре: на одной плате размещены восьмиканальный DWDM-мультиплексор/демультиплексор, усилитель и мультиплексор служебного канала. Пропускная способность трехъюнитовой системы достигает 2,4 Тбит/с на расстоянии до 100 км. Задействуются четыре длины волны, каждая из которых обеспечивает скорость 600 Гбит/с. Если у заказчика высокие требования к скорости, то максимальная емкость передачи по одной паре волокон может достигать 28,8 Тбит/с. Для этого необходимо использовать несколько таких систем и мультиплексор на 48 каналов. Высокоскоростная, многофункциональная система «три-в-одном» в компактном корпусе допускает каскадное соединение.

Фронтальную продувку системы охлаждения оценят специалисты, эксплуатирующие ЦОДы с холодным и горячим коридорами. Связь с внутренней сетью дата-центра обеспечат 12 клиентских портов 100G QSFP28, а в следующем релизе системы планируется поддержка 400GE QSFP-DD.

Выпускается и расширенный вариант системы – V6-DCI – высотой 6U со слотом для платы управления, шестью слотами для сервисных плат или пятью слотами для сервисных плат и слотом для усилителя. Максимальная емкость шасси – 4,8 Тбит/с (48 по 100 Гбит/с).

Помимо производительности и дальности существенный параметр для DWDM-систем – стоимость передачи трафика. У нового DCI-решения благодаря высокой производительности эта стоимость очень мала. По совокупности характеристик разработка российской компании – одно из лучших решений на мировом рынке компактных DCI-систем.

Другой важный момент – информационная безопасность. За рубежом сегодня идет ожесточенная борьба за использование систем локального производства. Так, в США на уровне правительства выделили огромные суммы на замену оборудования Huawei решениями местных производителей, а в Китае устанавливают DWDM-системы только собственной разработки. Единственный шанс обеспечить информационную безопасность страны – изготавливать оборудование самостоятельно.



Дело в том, что сложность проверки информации примерно пропорциональна скорости трафика. За десять лет скорость передачи по каналам связи выросла в 100 раз и во столько же выросла сложность контроля. Многие детали работы оборудования известны только вендорам. 100 Гбит/с означает полезную производительность канала, в действительности же может передаваться 120–130 Гбит/с, а разницу можно задействовать для нелегальной перекачки данных за границу. Никакие сертификации и проверки при использовании чужих систем не помогут, не дадут уверенности в отсутствии закладок и не устранят возможность кражи передаваемой информации. Тем не менее зарубежные компании на отечественном рынке связи доминируют, зачастую добиваясь успеха далеко не рыночными средствами. На мой взгляд, критически важно понимать, что только отечественные разработки в аппаратном и программном обеспечении могут гарантировать настоящую безопасность страны.

Время автоматизации и удаленного управления

Об интеллекте на границе, автоматизации и удаленном управлении – Юрий Драбкин, руководитель направления цифровой трансформации в регионах Южная Америка, Ближний Восток, Африка, Азия, Австралия и в странах СНГ подразделения Secure Power компании Schneider Electric.

– О цифровой трансформации говорят: спроси трех экспертов, получишь пять определений. Что цифровая трансформация значит для вас?

– Четкого общепринятого определения я не встречал. Для меня цифровая трансформация – это изменение основных операционных процессов заказчика и их непосредственная реализация с помощью ИТ. Если раньше ИТ использовались только для прикладных сервисов, таких как почта и доступ к файлам, или для автоматизации процессов ERP/MESH-систем, то теперь ИТ дополняют производственные и бизнес-процессы, являясь их основой и обеспечивая повышение эффективности основных сервисов заказчика. В медицине это диагностика и лечение заболеваний пациентов, в агропромышленном секторе – производство продуктов питания, в транспортной сфере – перевозка пассажиров, в логистике – доставка грузов и т.д.

– Что значит цифровая трансформация для самой Schneider Electric? Как меняется позиционирование компании?

– Приведу в качестве примера трансформацию производственных процессов. На наших заводах внедряется все больше ИТ-сервисов, средств автоматизации, технологий виртуальной и дополненной реальности. Полностью оцифровываются процессы сборки изделий, а сама сборка на цифровом уровне увязывается с другими стадиями – тестированием, поставками и пр. Такая трансформация – длительный процесс, но осуществляется глобально, в том числе на российских заводах.

Если говорить о позиционировании, то мы, как и многие компании, постепенно переходим к сервисной модели. Эта модель становится все популярнее у наших заказчиков. Например, в некоторых странах Европы ж/д-компании уже покупают не поезда, а сервис перевозки. Если сервис работает – компания-поставщик получает деньги, если нет – платит штрафы. Многие производители печатной техники предоставляют свое оборудование на сервисной основе. Привозят принтеры, а деньги берут за каждый отпечаток.

Schneider Electric развивает сервисную модель в отношении как отдельных небольших устройств, так и крупных технологических решений, например, для ЦОДов. В некоторых странах мира тестируется модель взаимодействия, когда мы предоставляем свои ИБП или даже edge-ЦОДы партнеру, который добавляет свои компетенции, ИТ-сервисы и дополнительное оборудование и все это предоставляет заказчику как конечный сервис на основе ежемесячной оплаты.

Кастомизировать и оптимизировать наши сервисные модели, снижать операционные затраты при предоставлении сервиса, повышать его качество и надежность нам помогает платформа EcoStruxure, которую мы активно продвигаем уже несколько лет.

– Как процессы цифровизации экономики меняют индустрию ЦОДов?

– Лет 10 назад мы все считали, что появится одно большое облако, и будет всем счастье. Но все оказалось гораздо сложнее. Есть широкий спектр задач, которые в централизованном облаке не решить. Например, сейчас все больше людей работает удаленно, в том числе используя видеоконференцсвязь. Выяснилось, что из-за задержек, гигантского объема трафика и пр. один, даже очень мощный, сервер ВКС на крупный регион не обеспечивает стабильность работы приложения. Чтобы все нормально функционировало, надо разбивать территорию на районы и в каждом устанавливать выделенный сервер. Другими словами, развивать сеть edge-узлов.

Другой пример: медицина. Аппарат МРТ выдает огромный объем данных. Часть данных необходимо первоначально хранить рядом с аппаратом МРТ, чтобы врач составил первичное заключение. Для этого нужен небольшой edge-ЦОД на месте. Далее данные передаются на уровень больницы – еще в один ЦОД, скажем, на несколько стоек, с медицинскими данными всех пациентов. Его ресурсами пользуются все врачи этой больницы. Архивы отправляют в центральный ЦОД, который может быть реализован на базе услуг colocation или в облаке. Получается иерархическая структура из разных по размеру и назначению дата-центров.

Так процессы цифровизации в экономике меняют ландшафт ЦОДов. Есть большие облачные гиперЦОДы, затем – мегаЦОДы для colocation, корпоративные дата-центры и, наконец, множество edge-узлов. Выстраивается новая гибридная система с гибкой подстройкой сервисов под каждого заказчика, под конкретную задачу его операционного процесса.

– Насколько распространение edge-ЦОДов изменит подходы к обеспечению надежности предоставления ИТ-сервисов?

– Несколько лет назад считалось, что все серьезные ЦОДы должны быть Tier III. Когда появилась концепция

Edge Computing, многие стали переносить те же требования на каждый edge-узел. Думаю, это неверно. Представьте ЦОД крупного ритейлера, который обеспечивает работу, скажем, 10 тыс. магазинов. Если возникнут проблемы в работе такого ЦОДа, то под угрозой окажутся все 10 тыс. точек, что критично. А если «упадет» edge-ЦОД в одном магазине, то да, этот конкретный магазин пострадает, но остальных такая авария не затронет. Необходимо взвешивать, какой уровень резервирования нужен в каждом конкретном случае.

Знаю примеры, когда в одном магазине ставят два-три одинаковых edge-узла – все без резервирования, но вместе они гарантируют бесперебойное предоставление ИТ-сервисов. Такую практику использует ряд наших заказчиков. В совсем маленьком магазинчике может быть один edge-узел. В более крупном – два-три узла, например, каждые четыре кассы обслуживаются своим edge-узлом. Когда один узел «падает», его нагрузку «подхватывают» другие. Кроме того, небольшие магазины «у дома» ночью не работают, так что всегда можно провести техническое обслуживание. Понятно, что требовать от подобных edge-ЦОДов ту же возможность обслуживания 24 x 7 без перерыва в предоставлении сервисов, что и от коммерческих ЦОДов Tier III, вряд ли разумно.

– А если не всем edge-ЦОДам необходим высокий уровень резервирования, то чем они отличаются от компьютеров, которые давно присутствуют рядом с кассами, стойками регистрации в аэропортах и т.п.?

– Edge-ЦОД обладает интеллектом для первичного анализа данных и поэтому не перегружает каналы связи и центральный ЦОД или облако. В этом его принципиальное отличие от «просто компьютера», который передает дальше все, что в него внесли.

Опять приведу пример, на этот раз нашу систему управления инфраструктурой EcoStruxure IT. Основа этой платформы – модуль, который собирает данные, EcoStruxure IT Expert. В составе этого «эксперта» есть шлюз, который устанавливается на Windows- или Linux-систему заказчика и агрегирует данные. Он же выполняет первичный анализ, наверх отправляет далеко не все. Если происходит какой-либо сбой, то шлюз сразу отправит все параметры. Если все нормально, то обобщенные данные могут пересылаться, скажем, раз в 15 минут.

При этом шлюз EcoStruxure IT Expert сопоставляет различные события. Предположим, есть ЦОД с двумя ИБП и 50 шкафами, в каждом шкафу по два PDU (два плеча подачи электропитания). В классической системе мониторинга, если отключится один ИБП, будет выдана информация о 51 инциденте (следом за отказом ИБП напряжение пропадет на 50 PDU). Шлюз разберется в ситуации: он покажет всего один инцидент – отказ системы электроснабжения площадки, в рамках которого произошли сбои 51 устройства. Вот вам пример интеллектуальной работы edge-узла.

– Цифровые платформы, как правило, неразрывно связаны с облачными сервисами. EcoStruxure IT тоже активно использует облака. Однако российские заказчики не торопятся отдавать в облака данные с критически важных объектов. Удается ли здесь достичь компромисса?

– Я работаю с заказчиками из разных регионов, и, конечно, есть страны, где заказчики намного охотнее идут в облако, чем в России. Но и в РФ есть отрасли, в которых заказчики используют облака не только для вспомогательных, но и для основных бизнес-систем.

Если говорить про EcoStruxure IT, то существуют как облачная платформа, так и вариант для установки у заказчика (on-premise). Мы всегда склоняемся к первому варианту, поскольку у него шире функционал. Big Data-аналитика уже сейчас помогает понять, какие элементы инфраструктуры выйдут из строя в ближайшее время. Сегодня глубокий анализ работы АКБ с прогнозированием доступен для наших однофазных ИБП Smart-UPS: когда батарея выйдет из строя, если ничего не предпринимать, какие действия необходимо предпринять, чтобы продлить срок эксплуатации АКБ (например, понизить температуру эксплуатации, сократить количество переходов на батарею, подстроив выходное напряжение источника в соответствии с сетью, и снизить число циклов разряда-заряда и т.д.), и самое интересное, каким станет предполагаемый срок эксплуатации АКБ в результате выполнения рекомендации. У решения on-premise такой модуль работы с Big Data отсутствует, но многие российские заказчики вполне успешно используют это решение. Хотя, мы надеемся, все больше компаний будут задействовать преимущества облачного варианта.

– Наблюдается ли в нынешних условиях рост спроса на системы удаленного мониторинга и управления?

– Рост числа сотрудников ЦОДов, работающих «на удаленке», привел к увеличению количества запросов на нашу систему EcoStruxure IT Expert. Важно отметить, что мы предоставляем возможность бесплатного тестового периода. Пожалуйста, подключайтесь к системе через сайт https://ecostruxureit.com/, пробуйте. Вся информация доступна на русском языке, для работы системы шлюзу нужен только доступ в интернет, а сам процесс регистрации, установки и настройки системы с нуля занимает всего от получаса времени. В целом можно говорить о многократном росте числа пользователей системы по всему миру за последние несколько месяцев.

Кстати, у тех площадок, на которых были развернуты системы удаленного управления на основе облаков либо с грамотно настроенным безопасным подключением по VPN для on-premise, сегодня нет сложностей с дистанционным доступом и выполнением большинства процедур, связанных с эксплуатацией ЦОДа. Да мы и сами активно используем нашу систему. Наши сотрудники служб эксплуатации тоже спокойно работают и контролируют все наши ИТ-процессы из дома.

Охлаждение ЦОДа: погружение неизбежно

Александр Барсков

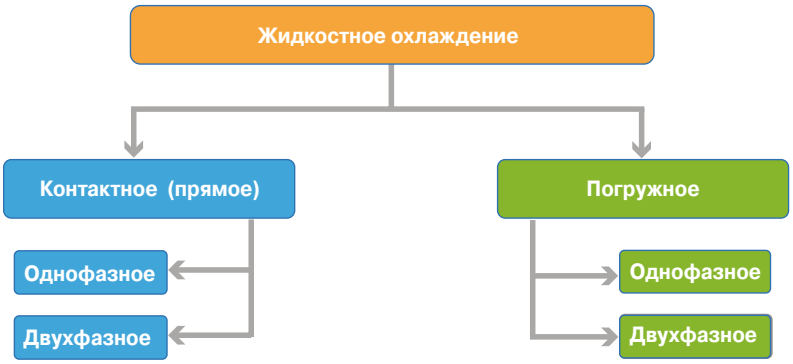
Ни рекордно низкий PUE, ни возможность многократного повышения мощности стойки не подвигли ЦОДы на использование жидкостного охлаждения. Однако неминуемый рост энергопотребления микропроцессоров заставит их обратить внимание на такие системы.

Жидкостное охлаждение – это не последний писк ИТ-моды, а самая что ни на есть классика, которой как минимум полвека. Первые системы жидкостного охлаждения появились в 60-х годах прошлого века вместе с мейнфреймами IBM System/360. Это была основная технология охлаждения, применявшаяся в вычислительных центрах тех времен. Заказчики доверяли жидкостному охлаждению, которое использовали для ИТ-систем, обслуживающих критически важные приложения.

Что же случилось с жидкостным охлаждением потом? Постепенно рынок завоевали относительно недорогие и маломощные серверы; они стали доминировать и в вычислительных центрах, которые во второй половине 90-х все чаще стали именовать центрами обработки данных, или дата-центрами. Для охлаждения не слишком энергозатратных микросхем таких серверов вполне хватало воздушного охлаждения – на процессоры устанавливали радиаторы и вентиляторы, как в обычных ПК. Более дорогое жидкостное охлаждение было практически забыто, его продолжали использовать разве что для суперкомпьютеров и кластеров высокопроизводительных вычислений (High Performance Computing, HPC).

Типовое решение для отвода тепла от ИТ-оборудования современных ЦОДов – воздушное охлаждение. Для этого задействуются либо шкафные (CRAH/CRAC), либо внутрирядные кондиционеры, подающие холодный воздух к

ИТ-оборудованию. Такие кондиционеры обычно используются, когда тепловая нагрузка на стойку составляет порядка 5 кВт. За счет изоляции воздушных потоков (коридоров) и ряда других специальных мер теплоотвод с одной стойки можно увеличить до 20 кВт. Но, по сути, это максимум, на который способны системы воздушного охлаждения. При увеличении плотности мощности охлаждение воздухом становится либо технически невозможным, либо экономически неоправданным.



▲ **Рис. 1.** **Классификация систем жидкостного охлаждения**

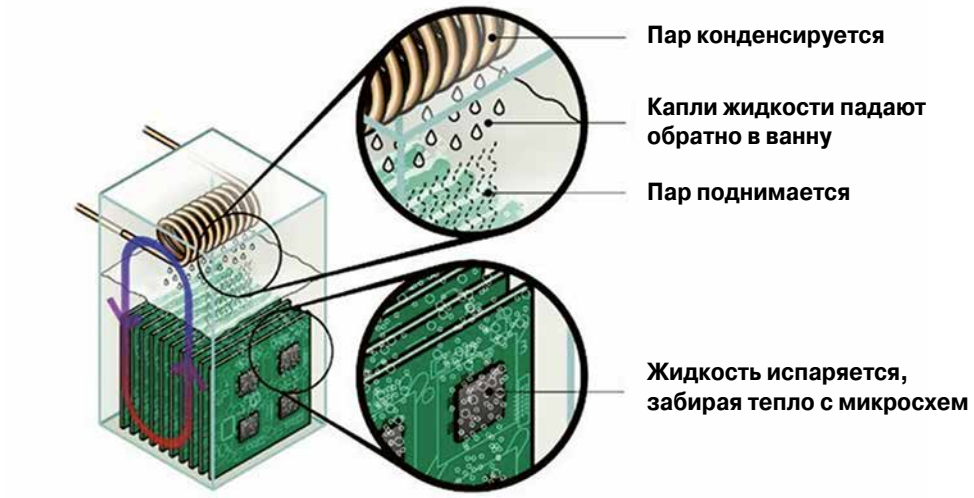
Таксономия жидкостного охлаждения

Множество различных способов жидкостного охлаждения можно разделить на две основные группы в зависимости от того, находится ли жидкость в прямом физическом контакте с охлаждаемой электроникой или нет (рис. 1). Если жидкость не контактирует непосредственно с электроникой, то такие технологии охлаждения, как бы это ни казалось странно, называют **контактными (conductive)**, если контактирует – то **погружными (immersive).** В системах первого типа обычно используют проводящие жидкости, например воду или ее растворы, в системах второго – диэлектрические жидкости: минеральные, синтетические масла или специальные инженерные жидкости.

Другой критерий классификации технологий жидкостного охлаждения основывается на том, претерпевает ли жидкость фазовый переход в процессе передачи ей тепла. Если фазового перехода не происходит, то технологию называют однофазной, если происходит, скажем, жидкость испаряется (рис. 2) – двухфазной. Вода и масла – однофазные охлаждающие жидкости. Многие хладагенты (например, R-134a) и некоторые инженерные жидкости (например, 3M Novec 7100) – это двухфазные хладагенты. Контактные и погружные технологии могут быть как однофазными, так и двухфазными.

Часто говорят **о прямом (direct) жидкостном охлаждении**. В этом случае имеют в виду контактное охлаждение, когда тепло электронных компонентов передается жидкости без привлечения воздуха. Пример такого решения – теплоотвод с помощью охлаждающей пластины, которая через термопасту присоединена к CPU (рис. 3). Прямое жидкостное охлаждение может использоваться для теплосъема с других электронных компонентов, в первую очередь оперативной памяти, контроллеров памяти и элементов системы электропитания. Важно не путать прямое (контактное) охлаждение с погружным: слово «прямой» здесь описывает непосредственную (прямую) передачу тепла жидкости, а не нахождение жидкости в прямом (физическом) контакте с электроникой.

В качестве альтернативы прямому жидкостному охлаждению может применяться и **гибридное (непрямое) охлаждение**. В этом случае тепло снимается с активных компонентов ИТ-оборудования воздухом с помощью тради-



◀ **Рис. 2.** **Принцип организации двухфазной системы погружного охлаждения на примере решения Allied Control (используется жидкость 3M Novec 7100)**

Источник: Allied Control

ционных средств, таких как воздушный радиатор. Затем нагретый воздух охлаждается в теплообменниках «воздух – жидкость», которые могут быть установлены как внутри серверов, так и за их пределами. Примером теплообменников «воздух – жидкость», которые располагаются вне серверов, являются так называемые холодные двери (Rear-Door Heat Exchanger, RDHx): в заднюю часть (дверь) монтажной стойки монтируется теплообменник, который, в свою очередь, подключается к трубопроводу с холодной водой чиллерной системы охлаждения здания.

Во многих случаях задействовать прямое жидкостное охлаждение для всех электронных компонентов в ИТ-оборудовании нецелесообразно или просто невозможно. Поэтому оставшаяся часть тепла (как правило, основная доля тепла отводится с помощью жидкостного охлаждения) выводится традиционными воздушными системами охлаждения. Этот смешанный режим охлаждения называют **комбинированным воздушно-жидкостным охлаждением**. Например, прямое жидкостное охлаждение может использоваться только для микропроцессоров, а традиционное воздушное охлаждение – для остальной электроники.

Во всех описанных выше способах охлаждения – прямого, гибридного и комбинированного – жидкость не находится в непосредственном физическом контакте с электронными компонентами. Далее в статье речь пойдет о более эффективных технологиях погружного охлаждения, когда жидкость находится в непосредственном контакте с электроникой.

Погружное охлаждение реализуется двумя основными способами. Первый – когда все устройство (сервер) погружается в резервуар (ванну) с диэлектрической жидкостью (рис. 4). В таком резервуаре, фактически лежащей горизонтально стойке, можно разместить до 42 серверных юнитов.

Второй вариант – размещение каждого вычислительного модуля в отдельном герметичном корпусе, заполняемом охлаждающей жидкостью. Такие серверы можно устанавливать в вертикальные стойки (рис. 5), для которых требуется меньше площади, чем для горизонтальных резервуаров.

В обоих вариантах погружных систем с помощью жидкости снимается 100% тепла, дополнительного (воздушного) охлаждения не требуется.

Время пришло!

Плотность мощности ИТ-оборудования постоянно повышается, а возможности систем воздушного охлаждения близки к своему пределу. Для отвода тепла от наиболее тепловыделяющих компонентов – CPU, графических процессоров (GPU), памяти – требуются все большие объемы холодного воздуха, генерация и

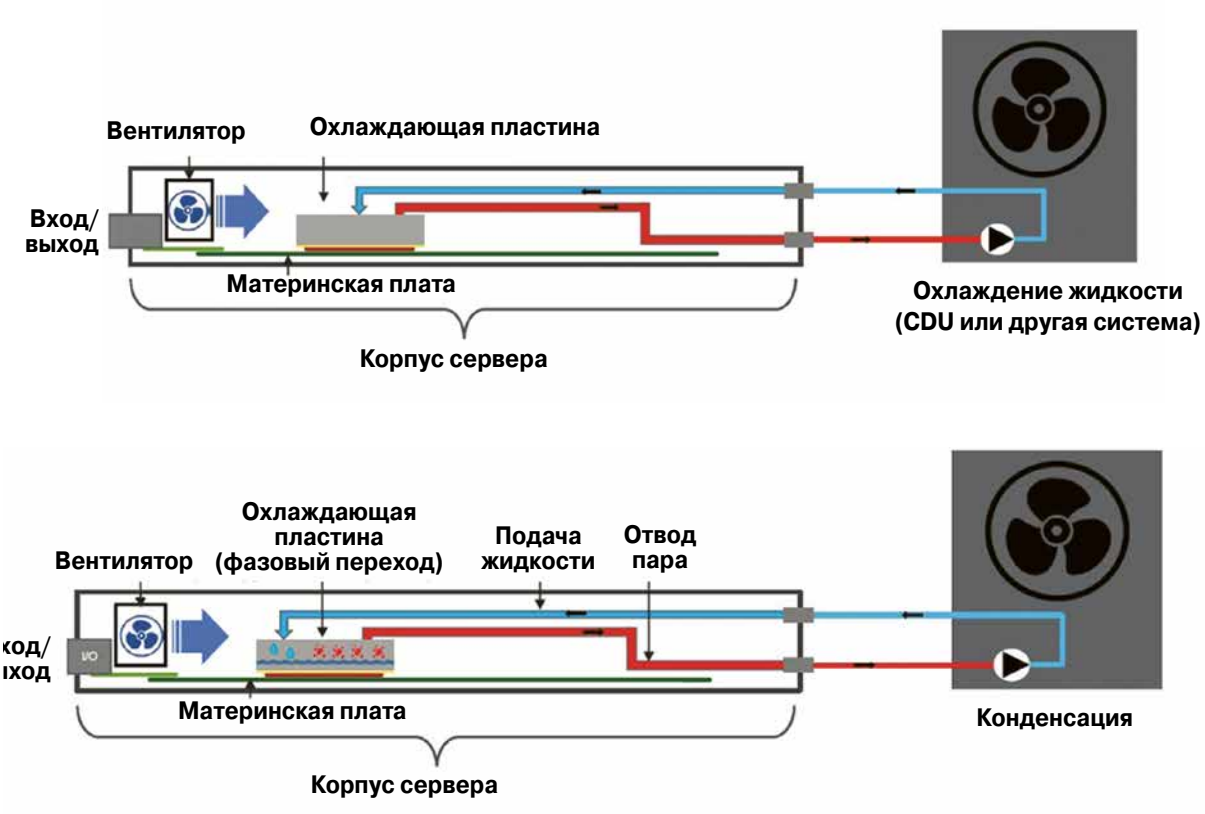


Рис. 3. ▶ Прямое (контактное) однофазное (вверху) и двухфазное (внизу) жидкостное охлаждение

Источник: Schneider Electric

◀ **Рис. 4.**
Решение, в котором серверы опускаются в ванну с охлаждающей жидкостью (система однофазного погружного охлаждения DTL)

Рис. 5. ▶
Стойка с серверами, каждый из которых размещен в герметичном корпусе, заполненном охлаждающей жидкостью

Источник: Iceotope Technologies

доставка которого становятся все более затратными. Более того, компоненты не только генерируют больше тепла, их число на единицу площади также увеличивается. На пути воздушного потока возникают все новые препятствия, для преодоления которых нужно увеличивать мощность вентиляторов. Кроме того, электронные компоненты, находящиеся в задней части сервера, заслоняются теми, что расположены спереди, – воздух до них доходит уже нагретый элементами, которые установлены ближе к входным вентиляционным отверстиям (вентиляторам).

Флагманские CPU и GPU ведущих производителей – Intel, AMD, Nvidia – уже давно преодолели уровень требований к теплоотводу (Thermal Design Power, TDP) в 200–300 Вт. И этот уровень постоянно растет. Так, анонсированные весной 2019 г. процессоры Platinum 9282 старшей линейки Xeon Platinum имеют TDP 400 Вт. С учетом установки нескольких процессоров в сервер высотой 1U получаем, что тепловыделение в расчете на 1U легко может составить несколько киловатт, а полностью заполненной стойки – 40–80 кВт.

Как уже говорилось, используя обычные методы воздушного охлаждения, практически невозможно отводить от стандартной ИТ-стойки более 20 кВт тепла. Для систем жидкостного охлаждения 20 кВт на стойку – далеко не предел. В настоящее время существуют системы, способные «снимать» 100 кВт, а некоторые – 200 кВт и более (в пересчете на типовую ИТ-стойку).

У внимательного читателя, наверное, возникнет вопрос: а зачем «запихивать» столько высокоплотной электроники в одну стойку, когда можно «разбросать» энергоемкие процессоры по нескольким стойкам, сохранив мощность каждой в пределах 20 кВт. Дело в том, что современные приложения, например искусственного интеллекта и анализа больших данных, требуют низкой задержки взаимодействия между процессорами и другими активными элементами. А значит, разносить на большие расстояния (даже по соседним стойкам) решающие одну задачу процессоры нежелательно.

Преимущества погружного охлаждения

Теплопередающие свойства жидкости обеспечивают на несколько порядков более эффективный отвод тепла от электронных компонентов. Жидкостное охлаждение позволяет плотнее размещать мощные процессоры и другие компоненты, а для отвода тепла от них требуется меньше энергии.

Расчет, проведенный экспертами The Green Grid, показывает следующее: чтобы устройство мощностью 1 кВт охладить на 11°C, потребуется поток воздуха 4474 л/мин или же расход воды всего 1,29 л/мин. Эксперты сравнили охлаждение стойки мощностью 20 кВт с помощью систем классического воздушного охлаждения и водяного охлаждения. Оказалось, что жидкостная система израсходует электричества примерно в 40 раз меньше (табл. 1).

В табл. 1 в расчет не бралась внешняя чиллерная система (или другая система, обеспечиваю-

Табл. 1.
Сравнение энергопотребления для охлаждения стойки 20 кВт (без учета чиллерной системы) ▼

	Воздушная система (вентиляторы)	Жидкостная система (насосы)
Мощность CRAH/CDU, кВт	2,4	0,1
Скорость потока для CRAH/CDU	90,6 куб. м/мин	2,57 л/мин
Мощность вентиляторов в ИТ-оборудовании *, кВт	1,5	0
Общая мощность вентиляторов и насосов, кВт	3,9	0,1
* Воздух поступает при 25°C		

Источник: The Green Grid

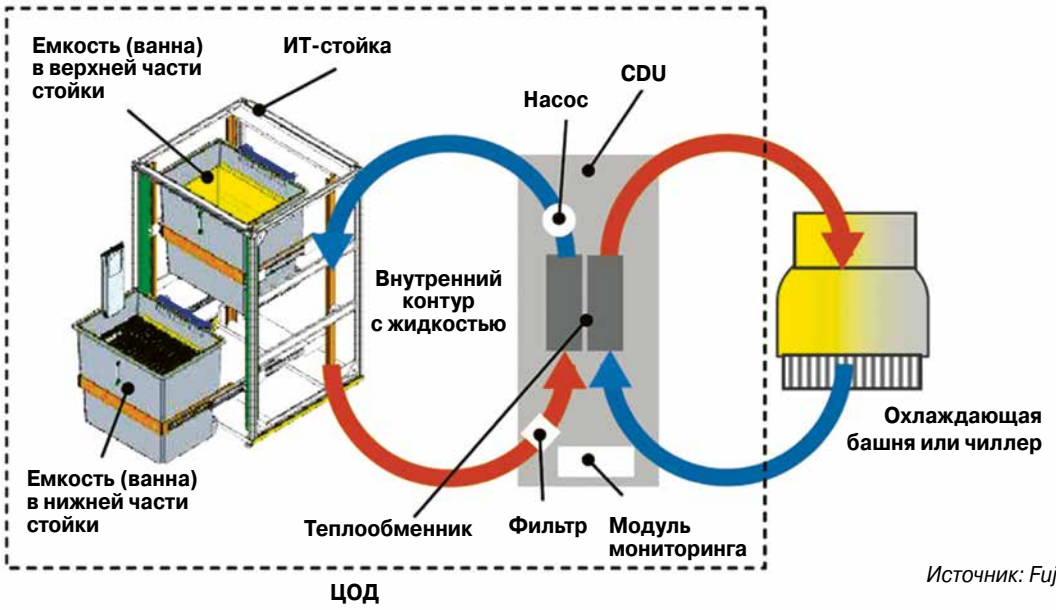


Рис. 6. ▶ **Интеграция системы погружного охлаждения (Fujitsu Liquid Immersion Cooling System) через блок CDU с внешним контуром охлаждения, подключенным к чиллеру или охладительной башне (драйкулеру)**

Источник: Fujitsu

щая охлаждение воздуха или жидкости, циркулирующей во внешнем контуре серверного зала). Система воздушного охлаждения серверного зала взаимодействует с такой системой через теплообменник «воздух – жидкость» в кондиционере CRAH. А система жидкостного охлаждения – через теплообменник «жидкость – жидкость» в распределительном блоке (CDU) (рис. 6). Как правило, CDU размещают непосредственно в конструктиве, где установлена и емкость с охлаждающей жидкостью.

В табл. 2 приведено энергопотребление сравниваемых систем охлаждения с учетом чиллерной системы. Также показан расход электричества для гибридной системы, когда 50% тепла с ИТ-оборудования снимается воздушной системой, а 50% – жидкостной.

Обратите внимание на то, какой расход воздуха (90,6 куб. м/мин) необходим для снятия 20 кВт тепла со стойки. Такой объем непросто обеспечить в серверных залах с типовым фальшполом, используемым в качестве воздуховода для подачи холодного воздуха к стойкам. Для этого потребуется создать высокое статическое давление воздуха в пространстве под фальшполом. Тогда как установить насос мощностью 100 Вт для прокачки 2,57 л охлаждающей жидкости в минуту совсем несложно.

Следует также заметить, что ввиду высокой эффективности систем жидкостного охлаждения они могут обеспечивать эффективный отвод тепла от электроники даже при высоких температурах охладителя: 45˚C и выше. Это позволяет отказаться от энергозатратных чиллерных систем, используя для охлаждения жидкости внешние системы естественного охлаждения окружающим воздухом, например, охладительные башни или сухие градирни.

В целом использование систем погружного охлаждения обеспечивает рекордно низкие показатели коэффициента энергоэффективности PUE (рис. 7).

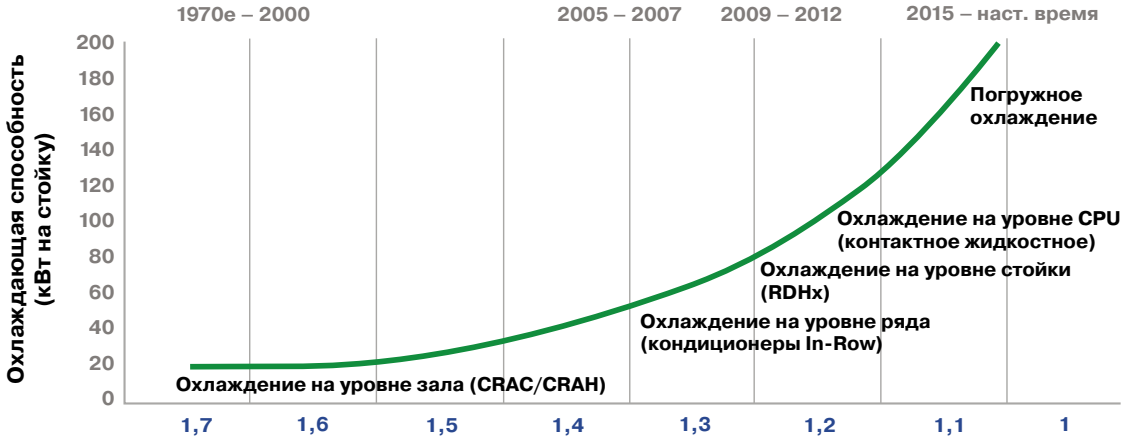
В дополнение к очевидным преимуществам существенной экономии места и энергии, погружное охлаждение позволяет также улучшить производительность и надежность работы ИТ-оборудования.

Более высокая производительность напрямую связана с более плотным размещением компонентов. Снижение задержки обусловлено как более короткими расстояниями между компонентами внутри сервера (стойки), так и улуч-

Табл. 2. ▶ **Сравнение энергопотребления для охлаждения стойки 20 кВт с учетом энергии, потребляемой чиллерной системой**

	Охлаждение воздухом (100%)	Жидкостное охлаждение (100%)	Гибридное охлаждение (50/50%)
Мощность вентиляторов/насосов оборудования в серверном зале, кВт	2,4	0,1	1,25
Мощность вентиляторов в ИТ-оборудовании, кВт	1,5	0	0,75
Мощность чиллерной системы, кВт	4,0	4,0	4,0
Общая мощность, кВт	7,9	4,1	6,0

Источник: The Green Grid



◀ Рис. 7. Эволюция систем охлаждения ЦОДов и снижение коэффициента PUE

Источник: Green Revolution Cooling

шенной общей пропускной способностью сети за счет меньших расстояний для подключения стойки к стойке и стойки к ядру сети ЦОДа.

Кроме того, нужно учитывать следующее: как только температура процессора повышается до максимально допустимой, его производительность необходимо снизить, чтобы избежать отказа из-за перегрева. Для работы с максимальной производительностью, что важно, в частности, для систем HPC, требуется, чтобы температура процессора и памяти оставалась низкой. Погружное охлаждение позволяет плотно упакованным системам работать непрерывно при максимальной тактовой частоте, избегая перегрева.

Поскольку жидкость имеет гораздо большую термическую массу (т.е. способность сохранять температуру при изменении внешних условий) по сравнению с воздухом, температура охлаждаемых с помощью жидкости компонентов более стабильна, что повышает надежность их работы. Кроме того, при погружном охлаждении нет потребности в вентиляторах. Это уменьшает или полностью устраняет вибрации, которые могут оказать негативное влияние на работу вращающихся дисков, а также на другие операции, например, на функционирование разъемных соединений в местах подключения коннекторов. Вибрации, возникающие при работе вентиляторов, могут вызвать ошибки чтения-записи во вращающихся дисках, что значительно снижает производительность операций ввода-вывода.

Решения, представленные на российском рынке

Основные игроки на мировом рынке систем погружного охлаждения – это американские (Green Revolution Cooling, LiquidCool Solutions, Midas Green Technologies), японские (Fujitsu, ExaScaler) и голландские (Asperitas, DownUnder GeoSolutions) компании, а также Submer Technologies (Испания), Allied Control (Гонконг), Iceotope Technologies (Великобритания), DCX (Польша) и Horizon Computing Solutions (Франция).

Однако большинство ведущих мировых производителей систем погружного охлаждения слабо представлены в России. В случае американских вендоров, даже при наличии у них российских партнеров (они есть, в частности, у LiquidCool Solutions), сложная международная обстановка и санкции серьезно затрудняют поставку их продукции российским заказчикам.

На нашем рынке давно работает японская Fujitsu, которая известна прежде всего как производитель серверов и систем хранения данных. Наличие в портфеле продуктов этой компании собственного, в том числе подготовленного для погружного охлаждения, ИТ-оборудования является ее серьезным конкурентным преимуществом как поставщика комплексных решений. Так, Fujitsu Liquid Immersion Cooling System представляет собой однофазную систему с жидкостью 3M Fluorinert, которая комплектуется серверами и СХД PRIMERGY мощностью до 60 кВт на стойку (см. рис. 6). Публичных кейсов по поставкам систем Fujitsu Liquid Immersion Cooling System в Россию нет, но известно об инсталляции в нескольких корпоративных ЦОДах.

Компания 3M активно продвигает на российском рынке технологии двухфазного погружного охлаждения с использованием негорючей неэлектропроводной фторсодержащей жидкости Novec 7100 (см. рис. 2). Построенные на базе этой жидкости системы предлагают как зарубежные поставщики (например, Allied Control), так и российские компании (TGE Group и Immersium). Российские партнеры изначально ориентировались на оборудование для майнинга, однако в настоящее время готовят решения для ЦОДов.

В уже реализованных проектах применение погружного охлаждения на основе жидкости 3M Novec 7100 обеспечивает отвод тепла до 3,5 кВт на 1U, при этом потенциал технологии – до 10–20 кВт. Одним из самых известных проек-

тов с использованием двухфазного погружного охлаждения на базе 3M Novec являются дата-центры BitFury Group, ведущего провайдера блокчейн-технологии. В них установлены системы охлаждения компании Allied Control (которая сегодня принадлежит BitFury Group).

На российском рынке активны и отечественные производители систем погружного охлаждения, предлагающие однофазные решения на базе жидкости собственной разработки. Так, компания DTL (специальный проект компании «Термосистемы») использует в своих системах диэлектрическую жидкость Cristallflow Dielectric. Серверное оборудование размещается в горизонтальных стойках (см. рис. 4), которые рассчитаны на мощность до 100 кВт.

Летом 2019 г. DTL объявила о запуске в эксплуатацию своего ЦОДа, использующего погружное охлаждение. Как заявляют в компании, это не только полностью коммерческий проект, но и демонстрационная площадка для знакомства всех заинтересованных предприятий, планирующих строительство или модернизацию дата-центров и серверных.

Liquid Cube – проект компании «Инпро Технолоджис» – представляет собой систему однофазного погружного охлаждения также на базе жидкости собственной разработки (рис. 8). Компания готова предложить «кубы» различного размера, при этом имеющееся решение на 23U обеспечивает теплоотвод 30 кВт – получается около 60 кВт в пересчете на типовую серверную стойку. Компания работает как с российскими, так и с зарубежными производителями серверного и другого ИТ-оборудования. Представители «Инпро Технолоджис» заверяют, что при достаточном объеме заказа вопрос сохранения гарантии на оборудование будет решен. Ряд зарубежных производителей сетевого оборудования уже обещали сохранить гарантию на свои решения при их работе в емкости с охлаждающей жидкостью Liquid Cube. Две системы Liquid Cube установлены в ЦОДе ФСК ЕЭС, но используются пока в тестовом режиме.

Рис. 8. ▶ Офисный вариант системы погружного охлаждения Liquid Cube

Еще одну отечественную систему однофазного погружного охлаждения предлагает компания «Иммерс», входящая в ГК «Сторус». Само решение (рис. 9) было разработано совместно с Институтом программных систем им. А.К. Айламазяна РАН. Компания «Иммерс» имеет более чем восьмилетнюю историю поставок высокопроизводительных вычислительных систем на основе погружного охлаждения на объекты Минобороны, МВД, Объединенной самолетостроительной компании, Авиационного комплекса им. С.В. Ильюшина, ТАНТК им. Бериева, Казанского авиазавода и т.д. (всего поставлено более 100 систем). Компания выпускает и серийные продукты, которые могут размещаться в ЦОДах. В решениях используется зарубежная и отечественная элементная база AMD, Intel, Nvidia, МЦСТ («Эльбрус»), «Норси-Транс» («Яхонт») и других производителей, с которыми возможно заключить соглашения о сохранении гарантии на серверы и отдельные модули.

Динамика роста…

По данным MarketsandMarkets Research, в 2019 г. мировой рынок систем погружного охлаждения составил $177 млн. По прогнозу аналитиков, в ближайшие годы этот рынок будет расти в среднем на 23,2% в год и к 2024 г. достигнет порядка $500 млн. Главными драйверами его роста в MarketsandMarkets Research считают увеличение плотности как микросхем, так и ИТ-оборудования в стойках, появление новых областей применения дата-центров, в частности развертывания вблизи источников/потребителей данных edge-ЦОДов, а также необходимость сократить расход электроэнергии на охлаждение ИТ-комплексов.

При этом рынок систем охлаждения для ЦОДов в целом до 2021 г. будет увеличиваться на 15%, а его ожидаемый объем к этому времени составит $14,28 млрд. Даже при самых высоких темпах роста сегмент погружного охлаждения в 2021 г. займет лишь порядка 2% рынка систем охлаждения для ЦОДов. Очень скромный показатель!

…и препятствия на его пути

Так почему же при всех своих многочисленных преимуществах системы погружного охлаждения пока не получили широкого применения, а используются в основном в единичных проектах для охлаждения суперкомпьютеров и HPC-систем?

Основное препятствие – консерватизм отрасли ЦОДов. Системы воздушного охлаждения давно и успешно применяются и де-факто ста-

ли стандартом в дата-центрах. Целое поколение технических специалистов выросло на таких системах, имеет большой опыт их инсталляции и технического обслуживания. Привыкли к ним и проектировщики, которые закладывают в проекты новых объектов хорошо им знакомые системы воздушного охлаждения.

Важное достоинство классических систем воздушного охлаждения – легкость и удобство обслуживания ИТ-систем, их модернизации, удаления и добавления в стандартные монтажные стойки. Подобного рода требования службы эксплуатации ЦОДов вправе предъявлять и к системам погружного охлаждения, и производителям важно обеспечить выполнение этих требований. Отговорки производителей, что, дескать, системы погружного охлаждения практически не надо обслуживать, выглядят неубедительно.

Тормозит внедрение погружных систем и то, что на практике средняя мощность стойки в российских ЦОДах увеличивается крайне незначительно. Этот показатель составляет 4–5 кВт. Более того, как утверждает ряд операторов ЦОДов, даже заказчики, купившие более дорогие стойки на 7–8 кВт, фактически загружают их на те же 4–5 кВт. Таким образом, одно из основных достоинств систем погружного охлаждения – высокая плотность мощности – не востребована российской индустрией ЦОДов.

Еще одно серьезное препятствие на пути использования систем погружного охлаждения – проблема их совместимости с ИТ-оборудованием. На данный момент большая часть серверов и другого ИТ-оборудования проектируется в расчете на воздушное охлаждение. В стандартных серверах много места занимают радиаторы, вентиляторы и воздушные каналы – элементы, которые не нужны при погружном охлаждении. Производители систем погружного охлаждения вынуждены сами убирать эти элементы. Но конструкции все равно остаются громоздкими. Технология погружного охлаждения позволяет использовать более компактное оборудование, и производители начинают предлагать продукты в более компактных формфакторах, однако такие решения пока не получили широкого распространения.

Сегодня мировые производители систем погружного охлаждения ориентируются больше не на стандартные серверы, а на высокоплотные системы: суперкомпьютеры, системы HPC, кластеры GPU с ускорителями Nvidia, узлы, усиленные ядрами FPGA или параллельными процессорами, такими как Intel Zeon Phi. Хотя ведущие производители систем погружного охлаждения заявляют о совместимости своих систем с ИТ-оборудованием основных поставщиков, его использование требует уже упомянутой доработки. На рынке пока мало серверов и СХД, готовых для погружных систем.

◀ Рис. 9. **МикроЦОД «Иммерс» на базе системы погружного охлаждения**

Отдельный вопрос связан с сохранением гарантии на серверное оборудование. Часть производителей готовы сохранять гарантию модернизированных серверов, если не превышается температура эксплуатации, не возникает перебоев в электропитании и не повреждены компоненты. Поставщики процессоров также могут сохранить гарантию, если температура процессора не превышала допустимых значений – без привязки к способу охлаждения. Но этот вопрос в каждом конкретном случае надо решать отдельно. И принятие положительного решения во многом зависит от объема заказа, а пока ИТ-системы на базе погружного охлаждения внедряются в единичных экземплярах, часто в тестовом режиме.

Перспективные применения

Основными областями применения погружного охлаждения являются сегодня специализированные решения, в частности суперкомпьютеры, системы HPC и высокочастотного трейдинга, комплексы майнинга. Однако уже в самое ближайшее время такое охлаждение будет все шире применяться в «обычных» дата-центрах, в первую очередь в облачных и edge-ЦОДах.

Вот некоторые перспективные сценарии применения систем погружного охлаждения в ЦОДах.

Быстрая организация edge-ЦОДа в сложных условиях. В местах, где размещают edge-ЦОДы, часто нет подходящей инфраструктуры, а среда эксплуатации экстремальна: высокая/низкая температура, высокие влажность и уровень загрязнений. Системы погружного охлаждения не требуют подготовленной инфраструктуры и нечувствительны к сложным внешним условиям. А контейнерные (модульные) решения на базе

погружного охлаждения позволяют реализовать edge-ЦОД за считанные недели. Причем в стандартный контейнер можно установить ИТ-системы мощностью сотни киловатт.

Размещение мини-/микроЦОДа в офисном помещении. Отсутствие вентиляторов делает работу ИТ-систем, погруженных в жидкость, практически бесшумной. Сама жидкость нетоксична и не представляет угрозы находящимся рядом людям. Наконец, для подключения микроЦОДа на базе системы погружного охлаждения требуется минимум инфраструктуры – только два канала для подвода и отвода жидкости. А высокая плотность мощности позволяет реализовать высокопроизводительную ИТ-систему в компактном корпусе, вписав его в интерьер современного офиса.

Наращивание ИТ-систем при отсутствии дополнительных ресурсов охлаждения, электропитания и/или свободной площади. Заменив стойки с воздушным охлаждением конструктивами с погружным охлаждением, можно кратно увеличить мощность ИТ-систем, используя имеющуюся на объекте инфраструктуру охлаждения, например чиллеры. При этом не потребуется больше электроэнергии, наоборот, ее экономия может достичь 50%. Дополнительная площадь также не потребуется.

Сокращение капзатрат на ЦОД. Построение традиционной системы охлаждения очень затратно: CFD-моделирование, выгородка коридоров, организация фальшпола, расходы на чиллеры, их обвязку, кондиционерные блоки в серверных залах и пр. – все это существенно удорожает создание дата-центров. По оценке Green Revolution Cooling, за счет отказа от компрессорных систем охлаждения (жидкость охлаждается по принципу фрикулинга) и повышения плотности размещения ИТ-оборудования системы погружного охлаждения позволяют до 50% сократить капитальные расходы на ЦОД.

Уменьшение подключенной мощности. Рекордно низкие показатели PUE системы погружного охлаждения дают возможность снизить общее потребление объекта до 50%. Это позволит владельцам/операторам дата-центров не только сократить эксплуатационные расходы, но и «вписаться» в лимит подключенной мощности, что особенно важно при создании ЦОДа в центральных районах мегаполисов, таких как Москва.

Основные тенденции на рынке ЦОДостроения – повышение плотности ИТ-оборудования при необходимости снижения расхода электроэнергии – делают системы погружного охлаждения все более востребованными. Поэтому такие системы неизбежно найдут свое применение в корпоративных и коммерческих дата-центрах. Для последних погружное охлаждение наиболее интересно при организации компактных и высокопроизводительных объектов под облачные платформы. ИКС

Выше температура – ниже PUE

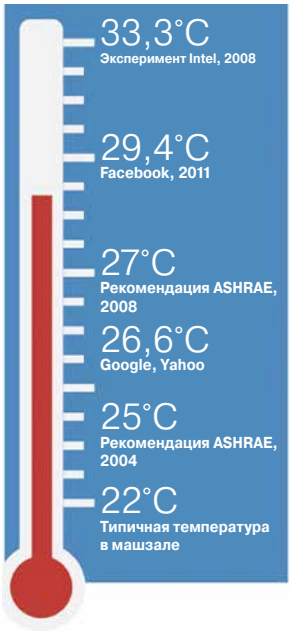
Виктор Прокофьев,
технический эксперт, ООО «Мицубиси Электрик (РУС)»

Повышение температуры в серверных залах – один из наиболее простых способов снижения операционных расходов ЦОДов. По данным агентства US General Services Administration, увеличение рабочей температуры ИТ-оборудования на один градус сокращает энергопотребление на 4%.

В течение многих лет идеальным для ИТ-оборудования считался диапазон температур 20–22°C (рис. 1). В 2004 г. Американское общество инженеров по отоплению, холодильному оборудованию и кондиционированию воздуха (ASHRAE), основываясь на своих исследованиях и рекомендациях производителей оборудования, рекомендовало диапазон рабочих температур от 20 до 25°C. Видя преимущество в снижении энергопотребления, проектировщики и операторы ЦОДов подняли температуру ближе к верхнему пределу 25°C.

В 2008 г. ASHRAE пересмотрело свои рекомендации и в приложении Environmental Guidelines for Datacom Equipment расширило рекомендуемый диапазон рабочих температур до 18–27°C. Инженеры ASHRAE указывают, что повышение рабочей температуры ИТ-оборудования мало влияет на рабочую температуру компонентов, но должно обеспечить значительную экономию энергии.

В 2008 г. Intel провела десятимесячный тест с использованием 900 серверов: 450 находились в традиционной кондиционируемой среде, а 450 охлаждались за счет наружного воздуха, без тонкой очистки и контроля влажности. Единственное условие заключалось в том, чтобы температура воздуха оставалась в пределах от 17,7 до 33,3°C. Несмотря на пыль, неконтролируемую влажность и большие перепады температуры, частота отказов серверов при отсутствии механического охлаждения оказалась всего на 2% выше, а экономия энергии достигла 67%!



◀ Рис. 1. Эволюция допустимой внутренней температуры в ЦОДах

В 2012 г. по результатам исследовательского проекта в Университете Торонто была опубликована статья Temperature Management in Data Centers: Why Some (Might) Like It Hot («Управление температурой в центрах обработки данных: почему некоторым (возможно) нравится погорячее»). Исследовательская группа изучила данные о надежности компонентов десятков ЦОДов. «Собранные нами данные говорят о том, что с учетом всех обстоятельств влияние температуры на надежность оборудования значительно меньше, чем принято считать, – отмечается в документе. – Повышение температуры ЦОДа создает потенциал для значительной экономии энергии и сокращения выбросов углекислого газа».

По результатам вышеупомянутых исследований и собственных экспериментов (попыток улучшения PUE) владельцам и операторам ЦОДов стало ясно, что в их интересах повысить рабочие температуры ИТ-оборудования.

Новая холодильная машина для современных ЦОДов

Расширенный рабочий диапазон

Для удовлетворения современных требований к системам ИТ-охлаждения, прежде всего – снижения энергопотребления и повышения надежности всей системы, компанией Mitsubishi Electric (MEHITS) была разработана новая холодильная машина (ХМ) с воздушным охлаждением конденсатора и функцией естественного охлаждения – NR-FC-Z. Данная ХМ способна работать при экстремальных климатических условиях: ее рабочий диапазон – от −30°C (−40° с опцией) до +50°C, конденсатор оснащен высокопрочным покрытием, машина способна выдерживать даже самые суровые промышленные или морские условия. NR-FC-Z имеет диапазон холодопроизводительности от 364 до 978 кВт: выпускаются 14 типоразмеров, доступных в двух вариантах эффективности и двух акустических исполнениях.

Увеличенные температурный перепад (ΔT) и температура хладоносителя (х/н)

Современное ИТ-оборудование готово для работы при температурах, превышающих традиционно принятые для серверных залов, что позволяет повысить эффективность системы охлаждения и снизить PUE ЦОДа. Охлаждающее оборудование развивается вместе с ИТ-инфраструктурой, поэтому машина NR-FC-Z была оптимизирована для работы с температурами 28°/20°C, обеспечивая более высокий КПД (EER до 4,1) и сводя к минимуму энергопотребление насоса благодаря специальной конструкции теплообменника, которая допускает пониженный расход х/н (ΔT до 11°C). ХМ NR-FC-Z уже сейчас способна работать при температуре выходящего х/н до 24°C.

▲ **Рис. 2. Использование режима «фрикулинга»**

Естественное охлаждение

Чем выше температурный график х/н, тем выше потенциал использования естественного охлаждения. Когда температура наружного воздуха падает ниже температуры обратного х/н, можно задействовать такое охлаждение. Холодильные машины NR-FC-Z работают в трех режимах:

- Механическое охлаждение. Общая холодопроизводительность обеспечивается компрессорами.
- Гибридное охлаждение. Температура наружного воздуха ниже температуры обратного х/н, режим «фрикулинга» включен, за счет него снимается часть нагрузки, остальная покрывается механическим охлаждением. Контроллер ХМ выбирает наиболее энергоэффективное сочетание работы обоих источников холода.
- Полное естественное охлаждение. Температура наружного воздуха достаточно низкая, чтобы полностью обеспечить поглощение теплоты в ЦОДе, компрессоры выключены. Данный режим обеспечивает максимальную экономию электроэнергии.

Благодаря увеличенным теплообменникам естественного охлаждения (драйкулерам) ХМ обеспечивает полную холодопроизводительность уже при температуре наружного воздуха 11°C при уставке по прямому х/н 20°C. Это означает, что значительную часть времени ХМ может удовлетворить потребности в охлаждении без использования компрессоров, т.е. работать с максимально возможной эффективностью.

В ЦОДе, расположенном в Лондоне, NR-FC-Z с рабочей температурой х/н 28/20°C может полностью удовлетворить потребность в охлаждении в течение 50% времени, используя только естественное охлаждение, и в течение 49% времени компрессоры работают при частичной нагрузке. Это означает, что 99% времени NR-FC-Z функционирует в режиме «фрикулинга» и крайне редко – как обычная ХМ (рис. 2).

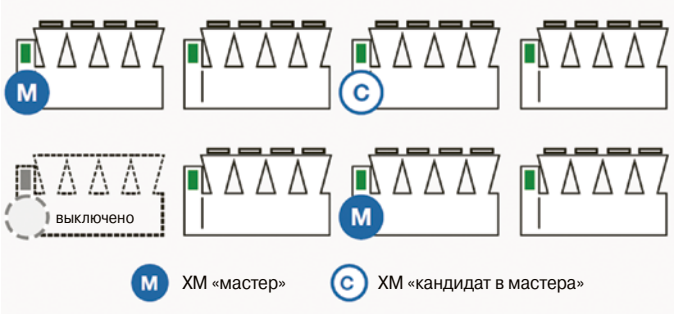
Оборудование для критически важных систем

Прерывание процесса охлаждения в ЦОДе может поставить под угрозу работу ИТ-оборудования и привести к серьезным экономическим последствиям. NR-FC-Z включает в себя полный спектр устройств и функций, которые обеспечивают максимальное время безотказной работы в чрезвычайных ситуациях. При сбое питания функция «Быстрый перезапуск» восстанавливает требуемую мощность охлаждения в кратчайшие сроки: ХМ мощностью 900 кВт достигает своей номинальной холодопроизводительности уже через 72 с. Кроме того, наличие АВР позволяет подключить устройство к двум отдельным линиям электропитания и автоматически переключаться в случае сбоя электроснабжения, что повышает уровень резервирования, надежность системы и дает возможность выполнять требования Tier III и Tier IV Uptime Institute.

Управление группой холодильных машин через ЛВС

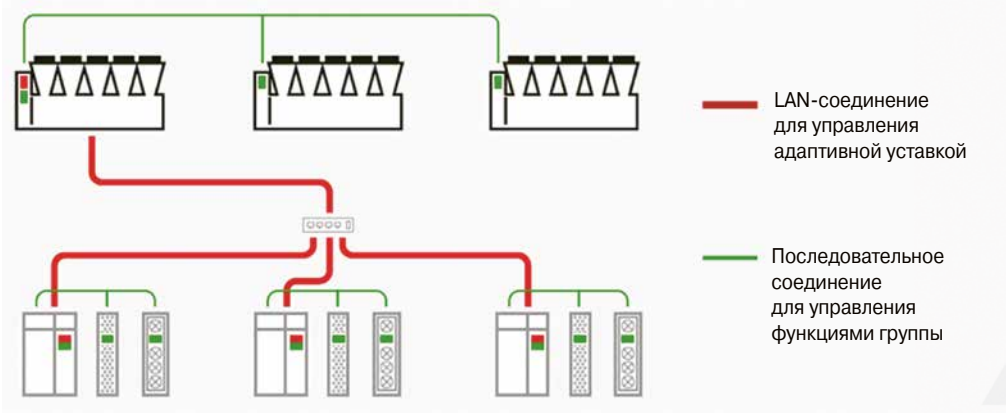
Встроенные интеллектуальные функции управления группой ХМ NR-FC-Z повышают эффективность и надежность системы и в значительной степени облегчают работу службы эксплуатации. В группу может быть подключено до 16 ХМ. Основные функции системы управления:

- «Динамический мастер» (Dynamic Master) с приоритетом назначения. Когда главная ХМ отключается, контроллер назначает другую ХМ в качестве главной, позволяя системе холодоснабжения продолжать функционировать. Инженер службы эксплуатации может заранее выбрать «кандидата в мастера» (рис. 3).



▲ **Рис. 3. «Динамический мастер» с приоритетом назначения**

- Распределение нагрузки между всеми ХМ в системе и последовательная загрузка машин.
- Управление приоритетом ресурсов в режиме гибридного охлаждения. Если в ЦОДе имеется несколько типов ХМ с разными технологиями, данная функция определяет приоритет использования каждой машины, соответственно распределяя нагрузку. Режим «фрикулинга», когда он доступен, всегда имеет приоритет перед включением любых компрессоров.
- Управление резервной ХМ.
- Быстрый перезапуск группы чиллеров.
- Адаптивная уставка. Контроллер координирует работу ХМ и внутренних потребителей, чтобы оптимизировать работу системы при частичной нагрузке. Каждая группа потребителей (до 20 групп) передает информацию о своей загрузке в режиме реального времени. Интеллектуальный алгоритм анализирует сигналы всех внутренних групп и при необходимости меняет уставки холодильной машины (рис. 4).



◀ **Рис. 4.** **Сетевое соединение для управления адаптивной уставкой**

Рис. 5. Принцип работы адаптивной уставки при частичной загрузке ▼

При полной нагрузке система работает с параметрами х/н 28/20°C, и внутренние блоки получают расчетный номинальный расход х/н. В традиционной системе с постоянным расходом при частичной нагрузке трехходовой клапан регулирует расход х/н через внутренний блок (и через байпас). С функцией адаптивной уставки трехходовой клапан прикрывает байпас, а контроллер XM повышает уставку (т.е. температуру выходящего х/н), в результате чего существенно снижается энергопотребление всей системы холодоснабжения (рис. 5). Благодаря этим функциям можно подключить более 300 установок (16 XM + 20 групп потребителей по 16 терминалов в каждой) без какого-либо внешнего оборудования и без дополнительных капзатрат.

Мобильный интуитивный интерфейс

Инновационная система KIPlink, использующая Wi-Fi, позволяет управлять XM со смартфона или планшета. Пользователь может включать и выключать устройство, регулировать различные параметры, настраивать функции локальной сети, отслеживать основные рабочие переменные, а также получать и сбрасывать аварийные сигналы. Кроме того, KIPlink может быть подсоединена к внутренней сети объекта по кабелю Ethernet, что позволяет инженерам обращаться к интерфейсу с использованием IP-адреса с любого устройства, подключенного к сети. С локальным мониторингом легче получить доступ к функциям управления без каких-либо ограничений с точки зрения безопасности. Для повышения уровня защиты KIPlink снабжена многоуровневой системой паролей.

Развитие высокотемпературных ЦОДов

Влияние повышения температуры ИТ-оборудования в ЦОДах на энергопотребление может значительно различаться в зависимости от архитектуры (топологии) системы охлаждения, климата, скорости вентиляторов и загрузки ИТ-оборудования. Необходимо четко понимать сложные взаимозависимости в структуре ЦОДов, а также анализировать и прогнозировать возможные риски и выгоды до того, как будут произведены изменения в проектировании и функционировании ЦОДов.

В ИТ-отрасли постоянно предпринимаются попытки повышения рабочей температуры в ЦОДах, а эксперты ASHRAE рекомендуют снижать их энергопотребление за счет увеличения количества часов функционирования режима естественного охлаждения. Но несмотря на усилия передовых инженеров, многие ЦОДы все еще работают при температуре не выше 21°C.

Хотя в проектировании ЦОДов существует консервативный подход (делать так, «как работает»), разработчики все чаще задаются вопросом, почему в новых проектах не всегда реализуется возможность повышения температуры приточного воздуха. При доказанной значительной экономии можно предположить, что число проектов, использующих повышенную температуру внутреннего воздуха, серьезно увеличится уже в ближайшее время.

Реконструкция ЦОДа: CAPEX, OPEX и здравый смысл

Александра Эрлих, генеральный директор, «ПрофАйТиКул»
Анна Васильева, руководитель направления ЦОД, «ПрофАйТиКул»
Михаил Казаков, руководитель проектно-технического отдела, «ПрофАйТиКул»

Разрабатывая проект реконструкции дата-центра, не следует забывать о том, что нередко CAPEX и OPEX выбираемых решений обратно пропорциональны друг другу, а дешевым оборудование некоторых производителей делается за счет снижения качества.

Объем данных, хранимых в ЦОДах всего мира, по оценкам портала Statista, только за период с 2016 по 2019 гг. вырос втрое. Всеобщая вовлеченность в цифровую жизнь требует все больше и больше вычислительных мощностей, и дата-центры за последние годы сильно изменились: увеличились нагрузка на стойку и плотность размещения стоек, стоимость ресурсов и возможности подключения и т.п.

Все это мы учитываем при проектировании новых ЦОДов, но как быть со старыми, уже действующими? Строительные конструкции и коммуникации можно эксплуатировать десятки лет, в то время как жизненный цикл серверного оборудования, даже при соблюдении всех требований производителя, составляет от трех до восьми лет (в соответствии с ASHRAE TC9.9 2016). Иными словами, ИТ-оборудование устаревает значительно быстрее, чем здание ЦОДа. Поэтому грамотная реконструкция отдельных систем с учетом особенностей существующего здания и коммуникаций будет наиболее рациональным решением.

Количество ЦОДов, нуждающихся в реконструкции, растет с каждым годом. Например, по статистике, в Германии в 2016 г. доля затрат на модернизацию дата-центров увеличилась на 33%, в то время как доля затрат на перенос данных в облака уменьшилась на 12% (рис. 1). В 2019 г. рост доли затрат на реконструкцию, согласно различным источникам, составил от 47 до 53%.

Итак, вы решили модернизировать свой старый ЦОД в соответствии с потребностями времени. Иными словами, заполнить его машзалы гораздо более высоко нагруженными стойками, по возможности сохранив действующие системы. Очевидно, что чем больше систем вы оставите без изменения, тем ниже будет CAPEX проекта. К сожалению, не со всеми системами можно так поступить. Одной из систем, сохранить которую в первоначальном виде, скорее всего, не удастся, является система холодоснабжения.

Конечно, первым возникает вопрос: менять старую систему на что-либо или дооснащать?

При дооснащении капитальные затраты невелики, вероятно, даже остановки ЦОДа не потребуется. Но, пообщавшись со своей службой эксплуатации, вы понимаете, что спасать уже, собственно, нечего. Техника устарела, такие модели больше не выпускают, запчастей и автоматики не найти. Значит, нужно идти на рынок.

Вы отправляетесь на отраслевой форум, семинар именитого поставщика или конференцию дистрибьютора многих поставщиков. После второго-третьего рекламного выступления, в котором вам рассказывают, что вендор X, У или Z лучше всех и каждый из них – мировой лидер, у вас складывается впечатление, что все они одинаковы, и пропадает желание слушать остальных производителей.

Один «размер» не подойдет всем

Другое дело – волшебный мир новых для вас инженерных решений. Тут и фрикулинг, безусловно позволяющий экономить электроэнергию, и охлаждение при помощи систем вентиляции, и бесчиллерные системы, и стена из воздухоохлаждающих приборов, и... глаза разбегаются. Что выбрать?

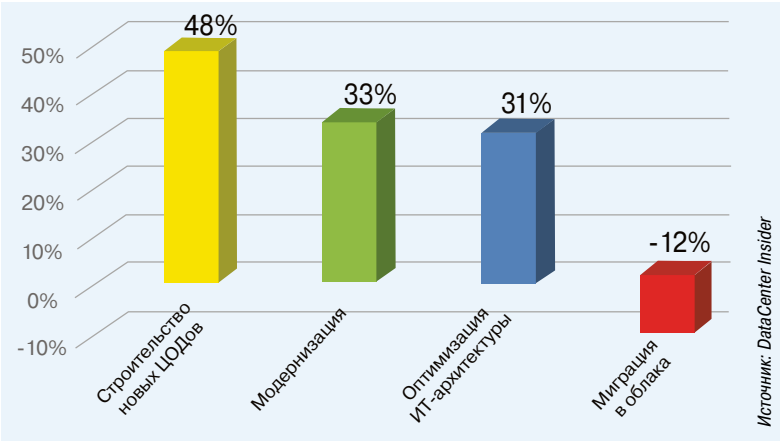
Вы начинаете расспрашивать знакомых, тех, кто недавно строил или реконструировал ЦОД. В большинстве случаев приобретенным опытом, зачастую очень полезным, они охотно делятся, особенно на фуршете. Обогащенные этим опытом, вы уходите с чувством, что теперь точно знаете, что делать.

Подвох кроется в том, что система холодоснабжения, которая прекрасно показала себя в одном ЦОДе, может совершенно не подойти другому. Просто потому, что у него меньшие электрические мощности без возможности их увеличения; другой климат; нет воды для прекрасной системы испарительного охлаждения или места для размещения отличных наружных и/или внутренних систем; недостаточная высота фальшпола, потолка или венткамеры и многое, многое другое.

Хорошо, если еще вы не успели потратить время и деньги на разработку бесполезной концепции и одумались сразу. Обиднее, когда приложили усилия, пытаясь приспособить чужую систему к своему ЦОДу, а она все равно не подходит.

На этом этапе вам скорее всего захочется все бросить и отказаться от идеи. Снести старое здание и построить на его месте новый современный центр обработки данных. Или вообще мигрировать в облака.

Но на самом деле реконструкция – весьма выгодное с экономической точки зрения мероприятие. Нужно только подойти к ней с нужной стороны.



▲ **Рис. 1. Изменение долей инвестиций в ЦОДы в Германии в 2016 г.**

Реконструкция ЦОДа отличается от нового строительства, по сути, только тем, что у нас уже есть здание, к которому проложены коммуникации, и известен объем ресурсов, таких как электроэнергия, которыми можно располагать. И эти особенности нужно учесть при разработке проектного решения.

Пожалуй, первое, что нужно сделать, – оценить перспективы роста мощности в течение следующих 3–8 лет. Далее необходимо проанализировать реализованные в мире решения и провести тщательный технический аудит имеющейся у вас инженерной инфраструктуры. В результате аудита вы сможете понять, что от старого ЦОДа останется в новом, а что непременно придется менять.

Наиболее трудоемкое дело – замена существующих коммуникаций. Если их пропускной способности достаточно для увеличенной мощности ЦОДа, то коммуникации лучше не трогать, как и систему пожаротушения. Хотя это и ограничит возможности изменения конфигурации залов.

Ключевой вопрос

А вот систему холодоснабжения, как мы уже говорили, вероятнее всего, необходимо будет менять и/или дооснащать. В России реконструкция ЦОДа осуществляется, как правило, спустя 10–15 лет после ввода его в эксплуатацию (иными словами, через 15–20 лет после начала проектирования).

Менять функционирующую систему, даже устаревшую, никому не хочется. Пусть она имеет свои недостатки, но об этих недостатках все известно, и с ними научились мириться. Но именно здесь допускается основная ошибка: при реконструкции в первую очередь рассматривают вариант замены компонентов существующей системы на новые и более производительные.

Подход в корне неверный. Вспомним о том, что увеличение ИТ-нагрузки влечет за собой совершенно естественное увеличение мощно-

сти отдельных компонентов системы и, как следствие, увеличение потребления и габаритов. Да, вы, безусловно, экономите на CAPEX; OPEX хотя и возрастает, но, как правило, лишь на величину энергопотребления. При стоимости электричества 1,5 руб. и даже 5 руб. за 1 кВт*ч на фоне всех остальных расходов увеличение операционных затрат на электроэнергию покажется вам незначительным.

Однако перед тем, как убедить себя в том, что найдено замечательное недорогое решение, прислушайтесь к здравому смыслу. Что вы будете делать, если не хватает электрической мощности и/или площади для установки, например, кондиционеров большего размера? Сокращать количество ИТ-оборудования для реализации устаревшего подхода к системе охлаждения? В чем тогда был смысл реконструкции?

Несмотря на то что в вашем случае стоимость электроэнергии, возможно, низкая, энергосбережение – это не способ сэкономить средства, а способ перенаправить имеющийся ресурс на получение дополнительной прибыли посредством размещения дополнительных стоек.

С опорой на мировой опыт

Обратимся к опыту Европы, США и ряда других стран, где строительство и эксплуатация ЦОДов имеют более долгую историю. Сегодня в мире функционируют ЦОДы с PUE 1,12, а среднеотраслевой PUE составляет 1,67 (по данным Uptime Institute за май 2019 г.). Существует масса решений, которые работают уже не один год и максимально реализуют потенциал энергосбережения за счет использования возобновляемых источников энергии, жидкостного охлаждения серверов, прямого или косвенного свободного охлаждения, переноса холодильного центра в подвальные помещения и пр. Среди этих решений наверняка можно найти одно или несколько, подходящих вам идеально либо требующих незначительных доработок.

При поиске решения, на которое вы будете опираться, разрабатывая свою концепцию, необходимо обратить внимание на такие параметры, как используемые ресурсы, климат внутри машинного зала, климат в регионе, в котором функционирует выбранный вами ЦОД-образец, на протяжении нескольких лет. Чем ближе эти параметры будут к вашим, тем больше у вас шансов получить схожие показатели работы в своем ЦОДе.

Выбор технологии

У энергоэффективных систем, например прецизионных кондиционеров на фреоне, CAPEX зачастую гораздо выше, чем у традиционных. Но зато вы получите отличный OPEX. А если вы решите обратиться к возобновляемым источникам энергии, то станете почти независимы от энергосбытовых компаний и стоимость электричества для вас будет минимальна. Но капитальные затраты такого проекта очень высоки.

При использовании прямого или косвенного фрикулинга важен температурный режим в машинном зале. Чем больше разница между температурой в машинном зале и температурой наружного воздуха (температурный напор), тем меньше CAPEX решения ввиду того, что необходимо совершить меньшую работу по переносу теплоты. Чем меньше температурный напор, тем большая работа требуется для охлаждения машинного зала, а это означает увеличение энергопотребления или площади теплообменной поверхности. Если мы совершаем работу за счет электроэнергии, то растет OPEX системы. Если увеличиваем теплообменную поверхность, то растет металлоемкость оборудования, т.е. CAPEX.

> Энергосбережение – это не способ сэкономить средства, а способ перенаправить имеющийся ресурс на получение дополнительной прибыли посредством размещения дополнительных стоек.

Рассматривая фрикулинг, особенно теперь, когда в европейской части России уже который год зима отнюдь не «русская», а «европейская», просто необходимо включать здравый смысл. Фрикулинг – это всегда высокий CAPEX, и окупается он только тогда, когда OPEX становится намного ниже. Иными словами, окупаемость такого проекта не должна превышать четырехпяти лет. Если же вы приобрели систему с фрикулингом, который начинается с 0°C или даже с отрицательных температур, то это дорогое решение, которым вы сможете пользоваться ко-

роткий промежуток времени либо не сможете пользоваться вообще. В таком случае ваша система не окупится и за 10 лет.

Размещение оборудования

Кроме климата и ресурсов при реконструкции ЦОДа нужно учитывать и другие ограничивающие факторы. Прежде всего необходимо понять, каковы возможности для размещения оборудования системы охлаждения именно на вашем объекте. Какой смысл рассматривать, например, систему прямого охлаждения, если существующие вентиляционные шахты не в состоянии пропускать необходимый объем воздуха?

Таких примеров можно привести множество. В нашей работе по реконструкции объектов разной сложности мы сталкивались с целым рядом ограничивающих факторов. Вот наиболее типовые из них: несущая способность крыши; места установки компонентов холодильных систем, в которые новое оборудование можно занести, лишь разобрав часть здания; невозможность увеличения пропускной способности фальшпола и/или вентиляционных шахт; отсутствие либо недостаточные площади смежных помещений.

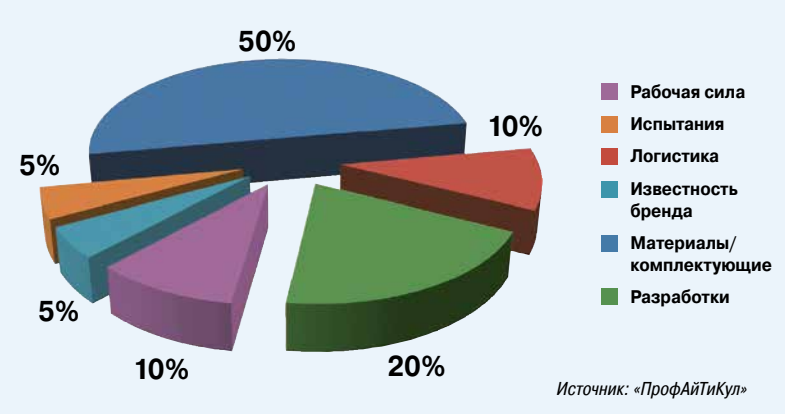
Зачастую выношенную красивую концепцию приходится оперативно менять исключительно из-за этих и им подобных факторов. Именно поэтому мы советуем не влюбляться сразу в одну концепцию, а остановиться на ряде понравившихся вам и подходящих по другим параметрам мировых образцов и затем незамедлительно провести аудит здания.

Выбор оборудования

В вопросе о том, на каком оборудовании реализовывать выбранное решение, снова вступают в игру три важных фактора: CAPEX, OPEX и здравый смысл. Как мы выяснили ранее, увеличение мощностей на OPEX повлияет незначительно, ведь зачастую более современные решения одновременно и более энергосберегающие. И вполне может получиться так, что по операционным затратам новая система от старой не отличается либо отличается незначительно.

Чего нельзя сказать о CAPEX. Не хочется сейчас пускаться в доказательства того, что энергоэффективные решения не всегда дорогие. Поговорим лучше о том, что цена одного и того же решения может сильно различаться в зависимости от выбранного оборудования.

Не секрет, что все оборудование, в том числе компоненты системы охлаждения (в рамках данной статьи мы говорим именно о ней), можно условно разделить на четыре класса: очень дешевое, дешевое, среднее и премиум-сегмент. Можно сколько угодно утверждать, что в стоимость дорогих брендов заложены расходы на маркетинг и поддержание имиджа бренда. Но давайте вспомним о том, что имидж – это отражение качества бренда. И в большинстве случаев премиальная цена все-таки означает премиальное качество.



▲ **Рис. 2. Структура стоимости оборудования систем охлаждения**

Раньше в мире ЦОДостроения первые два класса оборудования не рассматривались, их использовали в сегментах так называемого общегражданского строительства, где кратковременные отклонения от допустимых температурных режимов в 5°C, а то и 10°C не считаются критичными. Но затянувшийся экономический кризис, к сожалению, открыл для такого оборудования и сегмент центров обработки данных.

CAPEX системы на премиум-брендах может отличаться от CAPEX системы на дешевом или очень дешевом оборудовании на 30 и даже на 40%. Безусловно, такое процентное соотношение, переведенное в монетарное, всегда возбуждает желание «купить подешевле». Но именно в этот момент мы советуем обратиться к здравому смыслу.

Вспомните физику: для того чтобы получить работу, нужно затратить энергию. Для того чтобы изготовить более дешевое изделие, нужно на чем-то выгадать. Как производители компонентов систем охлаждения мы можем с уверенностью сказать: в стоимости климатического оборудования доля рабочей силы, задействованной непосредственно в производстве (в подсчет не входит гонорар работников отделов научных разработок и продаж), очень мала – не более 10% (рис. 2). Еще порядка 5% идут от известности бренда. Основную же часть стоимости изделия составляют вложенный в него интеллектуальный труд, методы испытаний и используемые при его создании материалы/комплектующие. Всего лишь урезав испытания на заводе, например, тестируя оборудование не по евро-

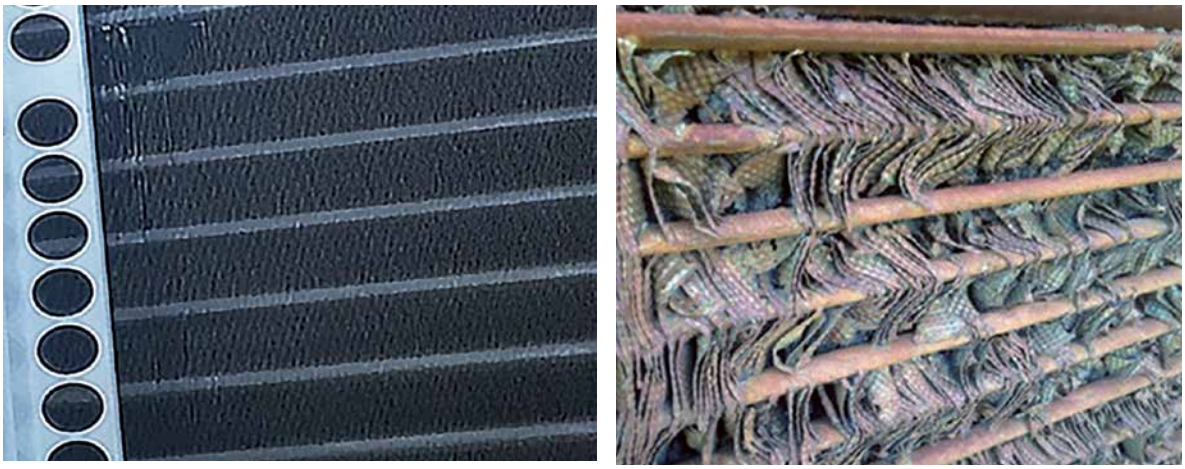


Рис. 3. ▶
Оборудование премиум-сегмента и дешевого сегмента спустя три года работы в сходных условиях

пейским нормам (EN), а по нормам ассоциации Eurovent, можно удешевить его на 5%. Доля материалов/комплектующих самая большая и составляет более 50% стоимости оборудования. Производители низкокачественных комплектующих появляются и исчезают каждые два-три года. Представляете, сколько можно выгадать на материалах/комплектующих? При этом затрат на научные разработки у дешевых и очень дешевых брендов почти нет. Производители этого сегмента не утруждают себя внедрением современных технологий, скопировать старое и утвердившееся на рынке гораздо дешевле.

Посмотрите на рис. 3: это фотографии оборудования премиум-класса и дешевого бренда (не самого дешевого), проработавшего в промышленной зоне со сходной картиной выбросов порядка трех лет. Правда, разница бросается в глаза?

> Единственная позиция, на которой можно получить экономию порядка 5–10%, не теряя при этом в качестве, – это оптимизация логистики.

Однако различная цена решений на премиум- и на дешевых брендах зачастую обусловлена не только качеством выбранных материалов, но и точностью и честностью инженерных расчетов.

Сколько бы эксперты рынка с трибун различных конференций ни говорили о том, что заявленные у многих производителей в технических листах параметры не всегда соответствуют реальности, соблазн «купить подешевле» часто толкает нас в пропасть нерабочих решений. Что мы имеем в виду? Не углубляясь в анализ термодинамических параметров (это тема отдельной статьи), поделимся своим опытом.

Заказчики любят сталкивать на тендере производителей лбами и часто предлагают «проанализировать» оборудование конкурента. Основная тенденция, которую мы замечаем в рамках такого анализа, – дешевые и очень дешевые производители в большинстве случаев лукавят с параметрами. Например, занизив температуру окружающего воздуха всего лишь на несколько градусов, можно предложить оборудование на 5–10% дешевле. А если такое «лукавство» затрагивает сразу несколько параметров, появляется возможность предложить на тендер оборудование, цена которого значительно более «конкурентная». А потом просто надеяться на то, что лето будет не слишком жарким, а зима не слишком холодной. Ведь по законодательству Российской Федерации гарантийный срок на оборудование составляет не более 18 месяцев, а его монтаж и пусконаладка зачастую начинаются не ранее года после изготовления. И дальнейшие проблемы с оборудованием легко можно свалить на другие компоненты системы, плохое хранение и прочие факторы.

Единственная позиция, на которой можно получить экономию порядка 5–10%, не теряя при этом в качестве, – это оптимизация логистики.

Оградить себя от недобросовестности можно, включив здравый смысл. Причем желательно делать это еще на этапе разработки концепции. Вспомните о том, что у вас есть собственная служба эксплуатации, а у ее сотрудников – огромный практический опыт. Пообщайтесь с ними, с другими участниками рынка. Не бойтесь задавать вопросы и потратить дополнительное время на анализ, это окупится сторицей бесперебойной работой вашего модернизированного ЦОДа.

Дальше дело за малым – нужно реализовать кропотливо разработанную концепцию. Но это уже другая история... ИКС

NEW

Rittal – The System.

Faster – better – everywhere.

Make IT Easy

Блок распределения питания (PDU): интеллектуальность и безопасность в IT

- Замена блока контроллера без отключения потребителей
- Каскадирование до 16 PDU в один порт коммутатора
- До 8 любых датчиков CMC III, включая LTE и СКУД

ENCLOSURES · POWER DISTRIBUTION · CLIMATE CONTROL · IT INFRASTRUCTURE · SOFTWARE & SERVICES

FRIEDHELM LOH GROUP

www.rittal.ru

RITTAL

Новые интеллектуальные PDU соответствуют современным требованиям дата-центров

С целью повышения отказоустойчивости ИТ-оборудования ЦОДов компания Rittal разработала новое поколение блоков распределения питания для телекоммуникационных и серверных шкафов.

Борис Васильковский, менеджер по продукции IT, Rittal

Отказоустойчивость в приоритете

Надежность обеспечения электроэнергией серверов, коммутаторов и другого активного оборудования ЦОДов зависит не только от наличия подводимых к дата-центру независимых линий электропередачи, ДГУ и аккумуляторных батарей, но и от распределения электроэнергии по стойкам телекоммуникационных и серверных шкафов.

Один из способов повышения отказоустойчивости вычислительной системы в стойке – использование серверного оборудования с двумя блоками питания, одновременно подключенными к двум линиям электропередачи. Причем для подключения активного оборудования все чаще применяются не простые розетки, а повышающие надежность работы распределители питания (Power Distribution Unit, PDU) с функциями удаленного измерения напряжения, потребляемой мощности, тока и других параметров электропитания.

Компания Rittal выпустила новую серию PDU, в которых используются высоконадежные автоматические выключатели и встроенные двунаправленные фильтры ВЧ-помех, которые не пропускают помехи от оборудования в сеть и от сети к оборудованию. В новых PDU установлены бистабильные реле, выдерживающие пусковые токи до 300 А. PDU защищает от искрения проводки – контроллер может «на лету» анализировать спектр протекающего по линии тока и отключать проблемную розетку.

Новая серия интеллектуальных блоков распределения питания PDU от Rittal снабжена контроллером мониторинга с расширенным набором интерфейсов, которые увеличивают возможности устройства. Отказоустойчивость контроллера PDU обеспечивается отдельным питанием по каждой из трех фаз, а также по PoE. Даже если питание пропадет на всех трех фазах, контроллер не отключится, а продолжит работу, высветив информацию о событии на своем цветном LCD-дисплее и послав сообщение о случившемся персоналу. Дополнительно отказоустойчивость системы повышает то, что замену блока контроллера в новых PDU можно провести в процессе работы без отключения потребителей.

Одна из тенденций в ЦОДостроении – увеличение температуры в машинных залах и использование высокотемпературных серверов. Новые интеллектуальные PDU Rittal с запасом удовлетворяют современным требованиям – они сохраняют полную работоспособность в диапазоне от 0 до 50°C. С некоторыми ограничениями по функциям PDU будут работать даже при температуре 60°C. Впечатляет и допустимый диапазон влажности – от 0 до 95%.

Свобода выбора конфигурации и простота монтажа

Для одиночных шкафов и небольших корпоративных серверных, где отсутствует необходимость в мониторинге, Rittal предлагает базовый вариант электрораспределения – блок без интеллектуальных функций **PDU basic**.

Интеллектуальные PDU оснащены контроллером. Удаленное измерение параметров энергопотребления по каждой фазе обеспечивают **PDU metered**. **PDU metered plus** проводят измерения не только по фазе, но и по каждой розетке. **PDU switched** снабжены бистабильными реле, позволяющими удаленно или по событию индивидуально управлять каждой выходной розеткой. Hi-end версия – **PDU managed** – измеряет параметры энергопотребления по каждой фазе, управляет каждой розеткой (до 48 шт.) в отдельности и по различным каналам оповещает об их состоянии.

Заказчик может выбрать готовые PDU, отвечающие его потребностям, из каталога, но разработанная компанией Rittal модульная концепция дает возможность индивидуального конфигурирования. В онлайн-конфигураторе на сайте Rittal можно не только подобрать PDU с необходимыми параметрами, но и выбрать цвет корпуса, изменить длину входного кабеля, штекер подключения, расположение дисплея – вверху или посередине. С Rittal можно согласовать индивидуальные требования к количеству и типу розеток, причем все три типа выходных розеток: C13, C19 и Schuko (евророзетка) – могут быть установлены в одном PDU. Также в PDU могут встраиваться съемный модуль защиты от перенапряжения и устройства измерения токов утечки.

PDU исключительно компактны – всего 44 мм в ширину, благодаря чему они могут устанавливаться между боковой стенкой шкафа и 19-дюймовой стойкой, не занимая дополнительного места. При наиболее часто встречающейся ширине шкафа 600 мм между стенкой и 19-дюймовым профилем встанут по одному PDU слева и справа, а в шкафу шириной 800 мм – по два. Кроме того, произвольное число PDU можно смонтировать непосредственно на каркасе шкафа. Широкий ассортимент крепежа обеспечивает возможность быстрого монтажа без инструментов или винтовые крепления в любые ИТ-шкафы. А в шкафах Rittal 19” ра-

ма специально оптимизирована для установки PDU, что позволяет за секунды провести монтаж и демонтаж этих устройств без применения инструментов.

Внутри шкафа – все под контролем

Благодаря улучшенному контроллеру новые PDU превращаются в развитую систему внутришкафного мониторинга, интегрирующую показания внешних датчиков и результатов измерений в самом устройстве для управления розетками и отправки оповещений. Контроллер имеет два резервирующих друг друга сетевых гигабитных Ethernet-интерфейса, разъем для подключения датчиков по CAN-шине, двухпроводной цифровой вход, интерфейс RS232, разъем USB для обновления конфигурации и просмотра журналов. Сухие контакты контроллера могут задействоваться для того, чтобы включить сигнализацию оператору. С помощью сухих контактов можно даже связать PDU разных шкафов, не используя сеть Ethernet, например, выполнить действие в серверном шкафу одного помещения по событию в шкафу в соседнем.

Интеллектуальные PDU позволяют подключить по CAN-шине до восьми элементов системы мониторинга CMC III, в том числе любые датчики – температуры, влажности, задымления, например, для отключения нужной розетки в случае возгорания блока питания сервера. К CAN-шине могут подключаться элементы СКУД, LTE-модуль, внешние устройства, например, сухие контакты кондиционеров или кнопка отключения питания на пульте оператора, системы аварийного открывания дверей и т.д. При этом PDU может отправить SMS или электронное письмо по заданным адресам с информацией об аварийном событии, связаться как с внешней, так и с внутренней (внутри шкафа) системой пожаротушения.

Например, если человек без права доступа попытается открыть серверный шкаф, то PDU может включить сигнал тревоги или отключить розетки. Настройки системы и уставки датчиков (предупреждение, тревога) настраиваются локально через USB-кабель либо удаленно через веб-интерфейс или консоль. Пример уставки: при значительном росте температуры в шкафу выключить розетки, при небольшом увеличении – послать сообщение администратору.

В зависимости от версии PDU могут реагировать на состояние сети питания, нагрузку на розетки, состояние датчиков, сигналы от различных систем оповещения сторонних производителей. Оповещения будут транслироваться через веб-интерфейс и по SMTP (электронной почте). Можно настроить оповещения через релейный выход, модуль LTE, в который вставляется SIM-карта оператора мобильной связи для отправки SMS-сообщений администраторам. Можно также использовать гигабитный сетевой интерфейс с поддержкой протоколов IPv4/v6, SNMP, OPC-UA, Modbus-TCP, а также HTTPS/SSH для связи с внешними системами мониторинга.

На каждом PDU новой серии теперь есть два Ethernet-порта. Один порт PDU можно подключить к коммутатору, другой – к следующему PDU и далее каскадировать, последовательно подключая PDU по Ethernet друг к другу. Таким образом, один порт коммутатора можно использовать для подключения 16 PDU, экономя дорогие порты Ethernet-коммутатора в

PDU исключительно компактны – всего 44 мм в ширину

ЦОДе. Для экономии IP-адресов PDU можно группировать по четыре штуки в систему master – slave с единым IP-адресом. При этом через веб-интерфейс три slave-PDU будут видны как устройства, подключенные к master-PDU.

Если количество PDU невелико, то с каждым можно работать через веб-интерфейс. В больших ЦОДах это неудобно. Целесообразнее задействовать системы мониторинга более высокого уровня – специализированные системы управления инфраструктурой дата-центра (DCIM) и зданий (BMS). Для интеграции PDU по SNMP в системы мониторинга инфраструктуры используются специальные базы переменных (Management Information Base, MIB), которые доступны для PDU Rittal. Актуальную базу MIB конкретного PDU можно скачать, подключившись к PDU по протоколу ftp.

Легкий переход на новые PDU

Для упрощения перехода на новые PDU компания Rittal разработала специальные таблицы, где для всех PDU предыдущего поколения подобран аналог из новой серии. На сайте Rittal (www.rittal.ru) для снимаемых с производства устройств традиционно указывается артикул замены: если нет желания работать с таблицей – можно ввести в поисковой строке на сайте артикул старого PDU и получить артикул нового. Такая же информация имеется и в электронной системе заказов, где для всех версий старых PDU будет предлагаться обновление. Перевод клиентов на новое поколение PDU стимулируется и ценовой политикой – несмотря на значительно расширившийся функционал, переход на новые PDU экономит средства заказчиков.

МикроЦОДы онлайн

Ответ компании C3 Solutions на пандемию – повышенное внимание к кадрам, перестройка бизнес-процессов и акцент на работу в режиме онлайн. Компания планирует существенно увеличить свою долю на российском рынке инженерного оборудования для дата-центров.

Мир резко изменился, обезлюдели улицы, сводки телевизионных новостей напоминают кадры фантастических фильмов-катастроф. Как работают российские компании при пандемии, что помогает в адаптации к новым условиям бизнеса – на вопросы нашего издания отвечает генеральный директор C3 Solutions Максим Кыркунов.

– Максим, как повлияла на функционирование компании пандемия?

– C3 Solutions продолжает работу, принимая все необходимые меры для обеспечения безопасности сотрудников. Весь фронт-офис переведен на «удаленку», на заводе ежедневно проводится медицинский контроль персонала, помещения обрабатываются ультрафиолетом и антисептиками.

Весна – время сезонного снижения спроса на нашу продукцию. Тем не менее по сравнению с прошлым годом мы отмечаем рост производства на 30%. Компания выполняет взятые на себя контрактные обязательства и осуществляет все запланированные поставки продукции.

– Что помогает компании успешно работать в такое трудное время?

– В первую очередь нам помогают своевременно проведенные преобразования. Можно сказать, что в 2020 г. C3 Solutions вошла другой компанией. Изменения коснулись продуктовой линейки, взаимоотношений с партнерами, расширения рынков. В результате улучшились финансовые показатели, за год вдвое выросла выручка.

Но самое главное – пересмотрены отношения внутри компании. 2019-й стал «годом человека C3» – человека нашей формации. Мы выработали собственную систему ценностей, единую этическую платформу. Вокруг этой платформы мы объединяем сотрудников и стремимся свой нравственный настрой транслировать участникам рынка, с которыми взаимодействуем.

Мы наладили HR-процессы. HR – это не только наем персонала и периодическая аттестация, но и адаптация вновь принятых людей к атмосфере в компании, к корпоративной культуре, сопровождение на протяжении всего цикла их работы на предприятии. Особенно важна HR-служба сегодня, когда из-за пандемии сотрудники испытывают стресс и нуждаются в поддержке.

В первом квартале 2020 г. мы перенастроили свою систему KPI. Сформулировали главный критерий: на 100% довольный клиент. Усовершенствовали систему мотивации персонала – разработали четкое соотношение трудового вклада каждого работника и материального вознаграждения.

Команда обновилась и усилилась, в частности, подразделение, которое занимается маркетингом и операционной деятельностью, выросло на 40%. В прошлом году мы перераспределили зоны ответственности, четко очертив для каждого круг обязанностей. Удалось объединить продажи и маркетинг, увязать исследование рынков с продажами. Операционная деятельность достигла уровня зрелости, пригодного для решения масштабных корпоративных задач.

– Какие новые решения появились в портфеле C3 Solutions?

– Несмотря на то что минувший год не был столь же богат на новинки, как предыдущие (фокус был сделан на дальнейшей адаптации наших микроЦОДов к запросам заказчиков), мы вывели на рынок систему мониторинга. В ней используются зарубежные компоненты, но собирается и настраивается система у нас. Решение протестировано у нескольких заказчиков и добавлено в наш портфель.

– Как проходит зарубежная экспансия компании?

– Мы укрепили контакты с зарубежными партнерами, повысили активность на общеотраслевых мероприятиях рынка дата-центров, специализированных конференциях, в том числе имеющих конкретную географическую привязку. В прошлом году объездили всю Среднюю Азию, где уже реализовали несколько проектов, вышли за Урал и с помощью партнеров занялись продвижением своей продукции в странах Восточной Европы.

– Как можно приобрести продукцию компании? Как быстро C3 Solutions реализует проекты на основе своих продуктов?

– Наша целевая аудитория включает и консерваторов, и новаторов, поэтому мы поддерживаем работу в разных форматах. Мы предоставляем традиционную консультационную поддержку по почте и по телефону, показываем решения в нашем демонстрационном зале, куда можно приехать, увидеть все своими глазами и оценить «на ощупь».

Для приверженцев новых технологий предлагаем онлайн-подход. На нашем сайте есть конфигуратор, с помощью которого можно подобрать необходимые компоненты решения самостоятельно. Добавлен даже элемент игры – раскраска микроЦОДа.

В конце 2019 г. мы пережили пиковый спрос на нашу продукцию, который удалось сгладить за счет более равномерного распределения заказов и переброски нагрузки на партнерские производственные площадки в России и за рубежом. Естественно, контроль качества выпускаемой продукции оставался (и остается!) за нами.

Проанализировав эту ситуацию, мы с партнерами пришли к выводу о необходимости расширения производства минимум в полтора раза в этом году и утроения производственных мощностей через два года. Все это делается для выполнения ключевого показателя – доставки решений заказчику в течение четырех недель, причем как по России, так и в Среднюю Азию.

У нас сформирован большой для нашего масштаба бизнеса склад, с которого в течение нескольких дней доставляем клиентам самые ходовые и критически важные решения. Важными потребителями являются коммерческие ЦОДы. Мы помогаем быстро, в течение нескольких дней, развернуть на их площадках вычислительную инфраструктуру заказчика.

– Как изменилась партнерская программа? Какие появились инструменты финансовой поддержки?

– Компания не взаимодействует с конечным заказчиком напрямую. Наша партнерская программа работает третий год, и за это время она показала свою эффективность. Сейчас программы обучения переведены в онлайн, в формат вебинаров. С нынешнего года начинаем проводить онлайн-сертификацию специалистов.

Не только мы, но и наши партнеры стали более зрелыми в части ведения бизнеса, стали серьезнее подходить к финансовым аспектам работы. Если раньше при выборе поставщика основную роль играла цена продукции, то теперь значение имеет и наличие финансовых инструментов, увеличивающих денежный поток компании. Мы разработали для партнеров набор финансовых инструментов С3 Finance, улучшающий финансовые показатели их проектов. В него входят различные схемы софинансирования сделок, отсрочки платежей со стороны ключевых дистрибьюторов.

– Как организуется гарантийная и постгарантийная поддержка решений?

– Наш подход к гарантийной и постгарантийной поддержке не отличается от традиционного, используемого зарубежными поставщиками. Правда, мы более терпимы к условиям установки наших решений по сравнению с зарубежными вендорами.

Стандартная гарантия 12 месяцев может пролонгироваться на требуемый заказчику срок. У нас функционирует сервисный центр, который принимает заявки на ремонтные работы. Стараемся расширять нашу сервисную партнерскую сеть, которая развивается быстрее и легче, чем сеть продаж. Поддержка сложных моделей даже для среднеазиатских проектов осуществляется из Москвы, поддержка простых изделий – силами местных партнеров. Главная цель – сведение к нулю времени простоя ИТ-сервисов, и этот принцип мы стараемся довести до каждого сотрудника. Вне зависимости от того, что произошло на объекте, мы сделаем все, чтобы партнеры и клиенты были удовлетворены эксплуатацией наших решений.

– Какова степень локализации продуктов? Появилась ли экосистема российских разработчиков?

– Подготовка к включению в реестр российских разработчиков находится в финальной стадии – документы представлены на рассмотрение Торгово-промышленной палаты. Процент локализации меняется в зависимости от сложности продукта – простые продукты локализованы практически полностью.

Вокруг С3 Solutions стала выкристаллизовываться экосистема партнеров. Если раньше закупки материалов производились без определенной системы, партии металла, например, закупались у разных поставщиков, то сейчас мы выбрали несколько ключевых игроков, с которыми организовали взаимодействие. В части физических компонентов система контрагентов уже сформирована и функционирует, в части программного обеспечения подбор разработчиков продолжается.

– На какие сегменты рынка ориентирована продукция С3 Solutions?

– Заходите на наш сайт – там информация о завершенных нами проектах постоянно обновляется. МикроЦОДы более востребованы в промышленном сегменте – горнодобывающей, обрабатывающей промышленности, атомной энергетике, нефтегазовом секторе.

Если говорить о традиционных изделиях: серверных шкафах, PDU, решениях для систем охлаждения с холодным и горячим коридорами, то их потребители – это крупные корпоративные клиенты и коммерческие ЦОДы, борющиеся за повышение своей энергоэффективности.

Продукты С3 Solutions – это функциональные аналоги лучших зарубежных решений, имеющие сопоставимое качество, но доставляемые в два раза быстрее и по существенно более низкой цене.

– Каковы планы дальнейшего развития компании?

– Команда объединена идеей взрывного роста. В плане финансовых показателей мы стремимся перейти в категорию крупного бизнеса. В этом году развернем программу С3 Finance и продолжим разработку новых продуктов. Шире будем задействовать онлайн-формат, чтобы партнер мог зайти на наш сайт, выбрать отвечающее его потребностям решение, разместить заказ, проверить его статус и получить без взаимодействия с человеком.

Когда ЦОДы становятся большими

Масштабирование систем бесперебойного и гарантированного питания, а также выбор технологии ИБП для мега- и гиперЦОДов – непростые задачи. Своими мнениями и рекомендациями делится Владислав Ротань, менеджер по развитию бизнеса компании Piller.

– Какие тенденции сегодня наблюдаются в области систем бесперебойного и гарантированного питания (СБГП) ЦОДов?

– В мировой практике четко прослеживается тенденция повышения энергоэффективности применяемых решений и надежности источников бесперебойного и гарантированного электропитания, минимизации воздействия на окружающую среду. Вместе с тем, по мере того как онлайн-сервисы делаются неотъемлемой частью нашей жизни, ЦОДы становятся все более коммодитизированными. Проектирование и строительство ЦОДов превратилось во что-то вроде конвейера, когда многим специалистам – как проектировщикам, так и заказчикам – самым простым выходом представляется масштабирование ранее апробированных решений: то, что хорошо работает в ЦОДе на 1 МВт, пытаются применить для площадок на 10, 20 МВт и т.д. Такой подход содержит много рисков.

– Да, ЦОДы становятся все крупнее. Каковы же особенности организации СБГП мега- и гиперЦОДов?

– За последние два года в России сразу несколько компаний начали проектировать и строить ЦОДы на тысячу и более стоек с планами масштабирования в два-три раза. ЦОД на 1 000 стоек – это инфраструктура СБГП примерно на 15 МВт.

Все большие статические ИБП, например на 1500 кВт, – это в явном или неявном виде сборные конструкции из нескольких источников меньшей мощности, поскольку их элементная база (IGBT-транзисторы) не позволяет создавать технически надежные и экономически оправданные ИБП единичной мощности свыше 600 кВт. За счет эффекта масштаба производства самый популярный «строительный блок» – это модуль ИБП на 250 кВт. Если вы видите статический ИБП на 1500 кВт, то это с большой долей вероятности комбинация 6 × 250 кВт. По этой причине решение на статических ИБП представляет собой большие массивы параллельно включенных типовых модулей по 150–600 кВт. Для экономии площади помещений, необходимой для размещения АКБ, все чаще рекомендуют использовать литий-ионные батареи.

Такой подход имеет свои недостатки: любое параллельное включение снижает надежность всей системы в целом, большое число установок требует дополнительных устройств коммутации и соединительных линий, а использование литий-ионных батарей увеличивает капитальные затраты и несет риски возможных пожаров. Предполагается, что недостаток статических ИБП, связанный с относительно низким показателем наработки на отказ (MTBF), компенсируется малым временем на их ремонт (MTTR) за счет возможности быстрой и «горячей» замены модулей ИБП. Но это спорное утверждение. Чем больше задействовано модулей, тем выше вероятность отказа и, что более важно, риск потери нагрузки в общей системе.

Альтернативным подходом в строительстве СБГП мега- и гиперЦОДов является применение моноблочных динамических ИБП (ДИБП) большой единичной мощности. Такие ИБП разделяются на дизель-роторные (ДРИБП), у которых дизельный двигатель подключается механическим образом к вращающемуся элементу конструкции (мотор-генератору, индукционному накопителю или маховику), и на роторные, у которых источники автономии (АКБ или маховик), а также ДГУ подключаются электрическим образом. Самые мощные ДРИБП выпускаются на 2400 кВт (для сети 50 Гц) – их ограничивает доступная мощность дизельных двигателей, тогда как роторные ИБП единичной мощности доступны в исполнении до 3240 кВт (например, модуль Piller UB-V 3240). Источником длительной автономии для столь мощных моноблоков могут быть, например, параллельно включаемые ДГУ или газопоршневые установки. Высокая мощность модулей ДИБП определяет меньшее количество единиц оборудова-

ния в системе СБГП, и с этой точки зрения роторные ИБП более привлекательны для применения в энергосистемах крупных ЦОДов.

– Вы представляете производителя, который выделяется на рынке тем, что предлагает и статические, и динамические ИБП. Для каких проектов вы рекомендуете ДИБП, а для каких – «старую добрую статику»?

– Действительно, Piller занимает особую нишу на рынке ИБП, поскольку производит и классическую «статику», и гибриды – «статику» с маховиками, и ДРИБП, и роторные ИБП, которые могут оснащаться как АКБ, так и маховиками. Понятие оптимальности является относительным и определяется требованиями заказчиков, которые наиболее часто обращают внимание на начальную стоимость решения (CAPEX), общую стоимость владения (TCO), надежность, занимаемое пространство, а также гибкость конфигурирования.

Большое преимущество статических ИБП – низкая начальная стоимость. Они могут оптимизировать КПД за счет «умного» отключения избыточных модулей, обладают большой гибкостью конфигурирования, но требуют много места для размещения АКБ, нуждаются в поддержании жесткого температурного режима и имеют срок службы до 15 лет. Более высокие, по сравнению с ДИБП, эксплуатационные затраты обусловлены необходимостью периодически менять АКБ и выполнять дорогостоящий ремонт с заменой силовых конденсаторов.

ДИБП выигрывают у «статики» в плане существенно более низких эксплуатационных затрат – например, в установках Piller замена подшипников требуется в среднем раз в 11–12 лет и выполняется непосредственно на объекте в течение двух рабочих дней. Если говорить о наших системах, то они занимают на 30–50% меньше места (по сравнению с СБГП на базе статических ИБП), обладают более высоким КПД (до 98% в онлайн-режиме) и способны работать при температурах до +50° С. Простая и прочная конструкция, исключающая силовые конденсаторы, обеспечивает очень высокую надежность: срок их службы – 20 лет и более. К недостаткам ДИБП можно отнести их относительно высокую стоимость и меньшую гибкость из-за большой мощности единичных модулей.

Если говорить совсем обобщенно, то решения на «статике» лучше смотрятся по CAPEX, тогда как ДИБП – по TCO. В ЦОДах мощностью 3–5 МВт первая же замена АКБ через 4–8 лет (в зависимости от выбранных батарей и режима эксплуатации) приводит к тому, что по TCO статические ИБП становятся дороже динамических. В более мощных ЦОДах, 10 МВт и выше, начальная стоимость решений на статических ИБП и ДИБП примерно одинакова, если считать всю инфраструктуру СБГП под ключ.

– Если сравнивать две основные системы накопления энергии – АКБ и маховики, в чем их преимущества и ограничения?

– Маховики более надежны, поскольку всегда известно их состояние. Они либо работают, либо нет, в отличие от АКБ, элементы которых могут отказать буквально на следующий день после успешного прохождения батарейных тестов. Времени автономии маховика 15–30 с достаточно, чтобы «переживать» кратковременные (1–5 с) пропадания внешней сети без пуска ДГУ, а также иметь запас времени на старт дизеля с третьей попытки и обеспечить гарантированный перенос на него мощности с маховика.

Если ЦОД оснащен современным ДГУ, то нет большой разницы, на какое время автономии выбираются АКБ – на 5 или 10 мин. Свернуть вычислительные процессы на серверах коммерческих ЦОДов за указанное время точно не получится. Фокус внимания при выборе источников автономного электропитания (АКБ или маховик) должен быть перенесен с длительности автономии на надежность таких источников. Чем больше мощность ЦОДа, тем больше элементов ИБП, АКБ, их параллельных цепочек и тем ниже общая надежность.

Применению АКБ нет альтернативы, когда нет возможности применять резервные генераторы либо существуют внутренние требования иметь длительную автономность от АКБ.

– Есть ли в вашей практике примеры, когда оптимальным оказывалось решение, сочетающее технологии (элементы) статических и динамических ИБП?

– Приведу два примера. В 2016 г. нами был реализован проект ЦОДа Hana Financial Group в Южной Корее общей мощностью 12,7 МВт. Впервые в мире была создана система энергоснабжения на базе конфигурации IP BUS N + 2 с применением ДРИБП и литий-ионных АКБ в качестве источника автономии. Заказчик получил более дешевое в показателях CAPEX и TCO решение, а также сэкономил 35% площади энергоцентра по сравнению с решением на статических ИБП.

Второй проект – российский. В настоящее время компания Selectel создает новые очереди ЦОДов в Москве и Санкт-Петербурге (по 5 МВт), система энергоснабжения которых реализуется на базе гибридных установок CPM300, построенных как классические статические ИБП с двойным преобразованием, но с маховиком вместо АКБ. Выбор заказчика был обусловлен экономией занимаемого пространства – порядка 40%, что позволило разместить энергоцентры в существующих зданиях, возможностью гибко наращивать мощность систем ИБП с шагом 300 кВт, а также более низким TCO.

– Сейчас, особенно в Европе, сильны экологические инициативы, что все больше затрудняет использование ДГУ. Быть ли ЦОДам без ДГУ?

– В России – скорее нет, чем да. Либо операторы ЦОДов должны использовать модель зеркалирования данных и процессов, имея географически разнесенные объекты, как это делает один известный российский поисковик, либо иметь надежный резервный источник, который может быть альтернативой ДГУ. Мир не застрахован от техногенных аварий. Вспомним блэкауты в энергосистеме России в 2005 г. из-за аварии на Чагинской ПС или в декабре 2010 г. из-за ледяного дождя, когда в некоторых районах электричество отсутствовало до двух недель. В мире, в частности в США и в Германии, высока доля автономной и альтернативной генерации, которая может выступать резервной сетью, чего нельзя пока сказать про Россию.

Беседовал Александр Барсков

Циркуляция масла в контуре. Проблемы и решения

Циркуляция масла в контуре холодильной установки – предмет споров и наиболее часто задаваемый клиентами вопрос при подборе оборудования. О том, как помочь маслу циркулировать правильно, рассказывает Сергей Зеленков, технический директор компании HTS.

Эффекты со знаком плюс и минус

На циркуляцию масла в холодильных установках оказывают влияние несколько факторов, один из которых – взаимная растворимость хладагентов и масла. Положительная сторона взаимной растворимости в том, что она обеспечивает смазку деталей компрессоров и способствует уплотнению динамических функциональных зазоров. Негативной же стороной является снижение кинематической вязкости масла, что уменьшает его смазывающую способность. При этом чем выше процент хладагента, растворенного в масле, тем ниже его смазывающая способность.

Каждый тип масла имеет свою характеристику растворимости в зависимости от температуры масла и давления хладагента (рис. 1).

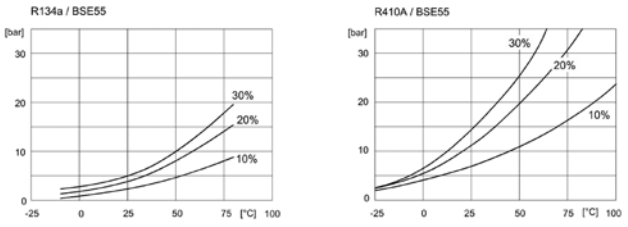


Рис. 1. Растворимость хладагентов в масле BSE55

Чем выше давление и ниже температура, тем растворимость фреона в масле выше. Помимо растворимости возможна смешиваемость – образование однородной среды из масла и хладагента в жидком состоянии. Для нас интересны в первую очередь так называемые разрывы смешиваемости – диапазоны температуры, в которых происходит расслоение (разделение фаз). Разрывы смешиваемости для масла BSE55 показаны на рис. 2.

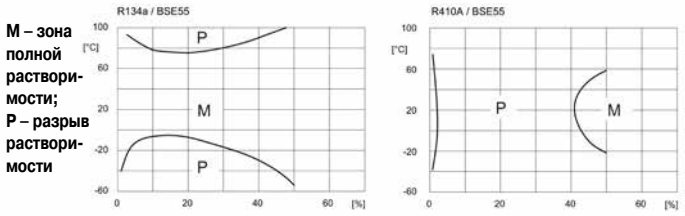


Рис. 2. Разрывы смешиваемости для масла BSE55: предельная температура в зависимости от массового процента масла в смеси хладагент – масло

Еще один негативный эффект – унос масла из картера компрессора в систему. Когда компрессор выключен, масло в картере абсорбирует некоторое количество хладагента, зависящее не только от температуры и давления, но и от процедуры остановки компрессора. При очередном старте компрессора в картере резко падает давление, что приводит к вскипанию хладагента, растворенного в масле. Масло в таком случае увлекается в большом количестве парами хладагента как в виде мелкодисперсных частиц, так и в парообразном состоянии. В результате в момент старта уносится самое большое количество масла.

По этой причине один из производителей рекомендует для своих компрессоров Copeland максимум 10 пусков в час. Количество пусков и остановок спирального компрессора ограничено только параметрами системы (тепловая нагрузка, температуры в помещении и на улице и т.д.). Минимальный промежуток между пусками зависит только от скорости возврата масла из системы после включения и складывается из времени уноса масла в систему при включении и времени возврата масла из системы и пополнения картера до необходимого уровня. Более частое включение компрессора, скажем, из-за большой тепловой нагрузки на испаритель, может привести к уносу масла из картера и повреждению компрессора.

Из компрессора во фреонопровод

Проследим путь смеси фреона и масла далее. После компрессора смесь попадает во фреонопровод. При движении рабочего тела по трубопроводу температура пара вследствие теплообмена с окружающей средой понижается, часть парообразного масла конденсируется и движется с потоком фреона в виде мелких капель. Размер частиц масла, унесенных потоком пара хладагента из компрессора, составляет 5–50 мк. Таким образом, масло, транспортируемое потоком рабочего тела по нагнетательному трубопроводу, находится как в виде пара, так и в виде капель – мелких, образовавшихся при конденсации парообразного масла, и более крупных, увлеченных потоком пара из компрессора.

Очевидно, что для нормальной циркуляции масла в системе скорость в трубопроводах необходимо держать минимальной как на стороне всасывания, так и на стороне нагнетания. Для газовых магистралей рекомендуются скорости 6–15 м/с, а для жидкостных не более 1,2 м/с. Разные источники дают разные значения оптимальной скорости движения хладагента, но все сходятся в том, что скорость на газовых магистралях должна быть выше скорости витания, а именно не должна падать ниже 2,5 м/с на горизонтальных участках и 7,5 м/с – на вертикальных.

Ключевая задача при выборе диаметров фреонопроводов – обеспечить циркуляцию масла (количество уносимого

масла должно равняться количеству вернувшегося) при допустимых потерях на сопротивление трубопроводов (сопротивление трубопроводов и элементов холодильной установки может значительно снизить ее холодопроизводительность с одновременным повышением энергопотребления).

Для интенсификации возврата масла линии фреонопроводов должны иметь уклоны (газовая магистраль – к конденсатору, жидкостная – к внутреннему блоку), а на вертикальных участках газовых магистралей следует устанавливать маслоподъемные петли. Допускается менять диаметры горизонтальных и вертикальных фреонопроводов.

У систем с переменным расходом хладагента можно встретить сдвоенное исполнение вертикальных участков (рис. 3). Это необходимо, чтобы предотвратить образование масляных пробок при работе с минимальной производительностью, когда скорости потока становится недостаточно для подъема масла.

Рис. 3. Дублирование вертикального участка фреонопровода

При таком исполнении диаметр малой трубы выбирается так, чтобы при минимальной производительности скорость потока в ней не падала ниже 5 м/с, а диаметр большой – так, чтобы при работе на полную мощность скорость в обеих трубах не превышала 20 м/с.

Типы маслоотделителей и их эффективность

Помимо проектных решений, связанных с прокладкой и выбором диаметров фреонопроводов, которые не всегда способны обеспечить нормальную циркуляцию масла, существуют механические способы отделения масла от хладагента. Так, в холодильной технике используются маслоотделители различных конструкций. Они предназначены для улавливания масла, уносимого хладагентом из компрессора, и сглаживания пульсаций нагнетаемого пара хладагента.

Маслоотделители делятся на промывные (барботажные) и инерционные (циклонные, сетчатые, комбинированные). Чаще всего встречаются маслоотделители инерционного и циклонного типа. Они устанавливаются на газовую магистраль между компрессором и конденсатором.

В инерционном маслоотделителе капли масла отделяются за счет резкого изменения скорости и направления потока. Эффективность такого решения, по данным разных производителей, составляет до 80%.

В циклонных маслоотделителях (рис. 4) установлена спиральная пластина. Поток пара поступает на нее и закручивается, при этом возникают центробежные силы, под действием которых капли масла отбрасываются к внутренней поверхности маслоотделителя, а затем стекают вниз. Эффективность данного устройства может достигать 99%.

Рис. 4. Циклонный маслоотделитель

Линию возврата масла подключают либо на сторону всасывания, либо через специальный регулятор уровня масла, устанавливающийся вместо смотрового глазка на картере компрессора. Первый вариант используется для компрессоров без смотровых глазков, второй вариант надежнее, но дороже.

При остановке компрессора часть горячего газа может конденсироваться внутри маслоотделителя, так как температура снаружи ниже, чем температура горячего газа. В результате уровень жидкости повысится, открыв тем самым поплавковый клапан, и жидкий хладагент может попасть в картер компрессора. Электронный регулятор позволяет этого избежать, открываясь только тогда, когда уровень масла падает внутри самого компрессора.

Унесенное хладагентом масло при неправильно спроектированных фреоновых магистралях, пройдя весь путь от компрессора до испарителя, может накапливаться в последнем и спровоцировать гидроудар. Избежать этого можно, установив на всасывающий трубопровод отделитель жидкости. Особенно это актуально в системах, где температура испарения и тепловая нагрузка на испаритель меняются в больших пределах, что может привести к заливу компрессора жидким хладагентом. Однако отделители жидкости не используют с зеотропными смесями (R407C), поскольку это может вызвать изменение их состава и увеличение температурного скольжения, а также в установках с функцией pump-down.

Наконец, стоит отметить, что уносимое масло образует тонкую пленку внутри трубопроводов и теплообменников, что препятствует нормальному теплообмену и снижает его интенсивность. Такое снижение наиболее заметно в испарителе, где благодаря низкой температуре масло и хладагент легко разделяются.

Итак, в большинстве случаев обеспечение нормальной циркуляции масла в системе сводится к грамотному проектированию фреоновых трасс. В некоторых случаях требуются добавление специальных устройств и настройка холодильного контура, что позволяет защитить компрессор и гарантирует, что масло не будет накапливаться в застойных зонах, предотвращая неизбежный гидроудар при их опорожнении.

Компания HTS, официальный дистрибьютор оборудования Stulz в России, всегда готова подобрать для своих клиентов оптимальные и надежные системы, основываясь на многолетнем опыте в решении непростых задач.

OpenRAN: дорогой верною?

Георгий Башилов, независимый эксперт

Внедрение технологий 5G – это не только рекордные скорости и минимальные задержки передачи данных, но и новые подходы к построению сетей сотовой связи, основанные на открытых стандартах.

Некоторые читатели, возможно, помнят времена, когда на разношерстном рынке персональных компьютеров, где бал правили «лабтамы», «амиги», «коммодоры», «атари» и другие самобытные устройства, появились компьютеры архитектуры IBM PC. Открытые интерфейсы и стандарты быстро сделали свое дело: ныне подавляющее большинство пользователей уже и не знают иных компьютерных архитектур. А некоторые – подзабыли и компанию IBM, по крайней мере как производителя ПК и ноутбуков.

Взаимозаменяемость отдельных компонентов настольных и все чаще мобильных компьютеров воспринимается сегодня как само собой разумеющаяся. Именно эта взаимозаменяемость и порождаемая ею конкурентная среда лежали в основе быстрого развития компьютерной индустрии и стремительного снижения цен на «мегабиты» и «мегагерцы».

Не исключено, что совсем скоро ситуация повторится на рынке сотовой связи: внедрение технологий 5G принесет с собой не только рекордные скорости и минимальные задержки передачи данных, но и новые подходы к построению операторских сетей.

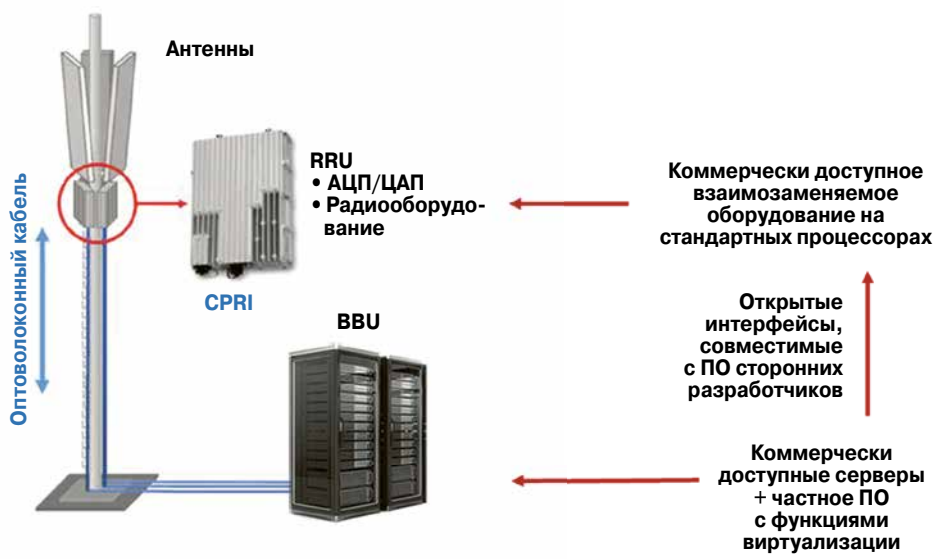


Рис. 1. Архитектура OpenRAN, основанная на принципах C-RAN ▼

Ах, эти… сотовые сети

Заметная часть установленных сегодня базовых станций построена в парадигме распределенной сети радиодоступа (Distributed RAN, D-RAN). В этой концепции базовые станции подключаются к ядру сети по интерфейсам PDH, SDH или Ethernet. Основу базовой станции составляет блок цифровой обработки радиосигнала (Baseband Unit, BBU), который размещается на земле, в непосредственной близости от сотовой вышки. Радиомодули (Remote Radio Unit, RRU) – их еще называют радиоголовками (Remote Radio Head, RRH) – устанавливают на вышке сотовой связи, в непосредственной близости от антенн.

Передача радиосигналов между BBU и RRU осуществляется через фронтхол (fronthaul), роль которого пару десятков лет исполнял коаксиальный кабель. Затухание в этом кабеле заметно ухудшало отношение сигнал/шум, надежность и качество связи. Замена коаксиала оптическим волокном, с одной стороны, привела к переносу функций оцифровки сигналов (АЦП/ЦАП) в радиомодули (и существенному улучшению параметров последних). С другой стороны, она сняла прежние ограничения на допустимое расстояние между модулями RRU и BBU. Определяющими стали задержки распространения сигналов и особенности радиопротоколов: как следствие, появилась возможность увеличить дистанцию между когда-то жестко привязанными друг к другу элементами базовой станции – BBU и RRU – до 20 и более километров.

От распределенной сети – к централизованной?

Сказано – сделано. Оптоволокно позволило объединить блоки BBU в едином центре цифровой обработки данных, что привело к распространению новой архитектуры построения сетей сотовой связи – C-RAN, впервые реализованной в 2010 г. на сетях China Telecom. При-

чем – сюрприз! – «C» в аббревиатуре C-RAN могло означать не только централизованную сеть радиодоступа (Centralised RAN), но и облачную – Cloud RAN. Эти понятия оказались тесно связанными и вместе определили новую архитектуру сетевого оборудования на узлах сотовой связи (рис. 1).

Перейдя к подключению радиомодулей с помощью оптоволоконного кабеля с его огромной пропускной способностью, операторы получили возможность не только разместить десятки блоков цифровой обработки в общих ЦОДах, но и использовать для задач специфической обработки радиосигналов коммерческое серверное оборудование, предлагаемое многочисленными производителями по конкурентным ценам. Высокоскоростной интерконнект с микросекундными задержками между серверами, на которых программно выполняются BBU, позволил «держать руку на пульсе» постоянно меняющейся, «дышащей» радиосети, предоставил возможность гибко распределять абонентов между базовыми станциями, обеспечивая им оптимальные условия приема и упрощая бесшовный роуминг между станциями.

Архитектура Cloud RAN дала возможность не только виртуализировать BBU и гибко управлять доступными вычислительными ресурсами, предоставляя их базовым станциям в соответствии с текущей нагрузкой (и плотностью абонентов) и минимизируя как энергозатраты на время простоя сотовой сети, так и потребность в самих вычислительных ресурсах. Последние получили возможность в определенных пределах «мигрировать» вслед за абонентами, снижая потребность в числе установленных серверов и, соответственно, затраты на развертывание сети.

Наряду с процессорами общего назначения BBU доступны ресурсы специализированных процессоров, реализующих задачи машинного интеллекта и цифровой обработки сигналов.

Подводя промежуточный итог, перечислим преимущества, которые принципиально отличают C-RAN от предыдущих сотовых архитектур:

1. Централизованная обработка радиосигналов сотовой сети. Благодаря виртуализации один сервер может обслуживать несколько RRH, а расстояние между радиомодулем и ЦОДом может достигать 15–20 км для сетей 4G (LTE/LTE-A) и 40–80 км для сетей 3G и 2G.

2. Возможность интеллектуальной обработки сигналов радиомодулей, входящих в общий пул, для уменьшения интерференции между базовыми станциями, управления нагрузкой на RRH и абонентскими подключениями, бесшовного переключения мобильных пользователей между зонами покрытия БС, повышения общей пропускной способности сети. Скорость передачи данных между BBU, входящими в пул, может превышать 10 Гбит/с, задержки и джиттер ограничены единицами и десятками микросекунд.

3. Виртуализация и управление ресурсами BBU на основе открытых платформ. Виртуализация ресурсов означает возможность их динамического распределения между базовыми станциями в зависимости от активности пользователей и, кроме того, отключения неиспользуемых BBU (а при определенных условиях даже RRH) для существенной экономии электроэнергии и снижения других операционных затрат. Блоки цифровой обработки построены на открытых программных платформах и серверах с открытыми архитектурами (x86/ARM/PowerPC/MIPS и др.) и объединены в пул стандартными высокоскоростными Ethernet-интерфейсами.

4. Возможность централизованного использования коммерческих спецпроцессоров для обработки сигналов и предоставления сервисов. В частности, в октябре прошлого года Nvidia и RedHat объявили о совместном продвижении решений, основанных на RedHat Open Shift и платформе суперкомпьютерных вычислений Nvidia EGX, на телекоммуникационных рынках и прежде всего для сетей 5G.

5. Быстрое развертывание новых сервисов на базе открытого ПО и пулов BBU. Оператор независим от производителя оборудования BBU и может разрабатывать и предоставлять новые виды услуг самостоятельно или с помощью внешних интеграторов.

Ethernet повсюду

Казалось бы, все в шоколаде – и операторы, и производители должны быть довольны. Но нет: узким местом в столь замечательной картине оказался интерфейс CPRI (Common Public Radio Interface – общий открытый радиоинтерфейс) между RRU и BBU. Его разработка осуществлялась совместно ведущими производителями телеком-оборудования с целью стандартизации производства специализированных микросхем и снижения стоимости оборудования. Однако, несмотря на обещающее название (общий открытый), нюансы в реализации CPRI привели к несовместимости решений разных производителей. Кроме того, стандарт CPRI предполагал максимально простую структуру и функциональность радиомодулей, ограниченную АЦП, ЦАП и усилителями СВЧ, и использование отдельных лямбд или волокон на каждый из каналов MIMO. Следствием стала повышенная нагрузка на оптический фронтхол и крайне неэффективное использование оптических каналов.

На решение проблем роста нацелен «улучшенный» стандарт CPRI (enhanced CPRI, eCPRI). Возможно, более точной была бы расшифровка Ethernet CPRI, но обо всем по порядку.

Прежде всего, eCPRI соответствует открытым стандартам и, как подтверждают первые внедрения, обеспечивает взаимозаменяемость радиомодулей разных производителей. Кроме того, eCPRI разгрузит BBU от задач обработки многоканальных сигналов MIMO, уже только этим снижая нагрузку на сеть.

Среди других преимуществ eCPRI:

- независимость от реальной топологии транспортной сети, выполнение поверх транспортного уровня;
- использование для подключения RRH стандартных Ethernet-коммутаторов и интерфейсов 10G/100G Ethernet;
- возможность использования Ethernet-коммутаторов независимых производителей на трассе между ЦОДом и радиомодулем;
- решение задач избыточности, безопасности, качества связи и т.д. стандартными средствами Ethernet-протоколов, в том числе приоритизация трафика eCPRI для уменьшения джиттера и задержек;
- возможность наряду с кадрами eCPRI передавать в реальном времени другие виды Ethernet-трафика.

Таким образом, внедрение eCPRI потенциально способно не только снизить нагрузку на оптический фронтхол оператора и устранить прежнюю зависимость от производителей радиомодулей. У оператора появляется возможность сочетать фронтхол и транспортную Ethernet-сеть в единой сети доступа и гибко модернизировать сеть с использованием лучших на данный момент решений.

Более того, универсальная (фронтхол поверх транспортной сети) архитектура eCPRI позволяет предоставить абонентам на прежней фронтхол-сети услуги не только мобильного, но и фиксированного доступа. В том числе беспроводного, на скоростях несколько гигабит в секунду. Напомним, в миллиметровом диапазоне длин волн клиентам становятся доступны недорогие гигабитные каналы «точка – точка». Зачастую такие линии строятся на модифицированном оборудовании 802.11ad. А стандарт 802.11ay, принятие которого ожидается уже этим летом, обещает дать операторам возможность развертывать гигабитные mesh-сети фиксированного доступа в диапазоне 60 ГГц (рис. 2). Сходное оборудование может применяться и для подключения по беспроводным каналам самих радиовыносов.

К слову, если вы гуляли по вечерней Москве, наверняка заметили, насколько красивой делает ее подсветка зданий, подчеркивающая и раскрывающая архитектурные формы и наполняющая старые районы неповторимым очарованием. Так вот, каждый светильник таких зданий – отличное место для установки беспроводного миллиметрового RRU.

Стандарты

Разумеется, все эти «молочные реки с кисельными берегами» будут невозможны без жесткого соответствия стандартам. Стандартизацией решений для сетей радиодоступа, основанных на архитектуре C-RAN с использованием протокола eCPRI, занимаются сегодня несколько комитетов, включая:

- OpenRAN (в рамках более масштабного проекта Telecom Infra – развития открытой телекоммуникационной инфраструктуры, продвигаемого компанией Facebook);
- O-RAN – консорциум, образованный в феврале прошлого года пятью ведущими мировыми телеком-операторами: AT&T, China Mobile, Deutsche Telekom, NTT DoCoMo и Orange.

Собственные национальные стандарты и соответствующее им оборудование разрабатывают в России, Индии, Китае, Вьетнаме и множестве других стран.

За последние несколько месяцев вопрос из технологической плоскости сместился в политическую: обеспокоившись стремительным развитием Huawei, США ввели запрет на использование в стране оборудования этой компании стандарта 5G, лоббируют запреты в других государствах и инвестируют миллиарды долларов в разработку национального оборудования 5G OpenRAN.

Несмотря на кажущееся обилие альянсов и ассоциаций, можно отметить слаженность усилий разных игроков: некоторые из них участвуют сразу в нескольких комитетах стандартизации и при всей сложности стоящей задачи заинтересованы во взаимной совместимости выпускае-

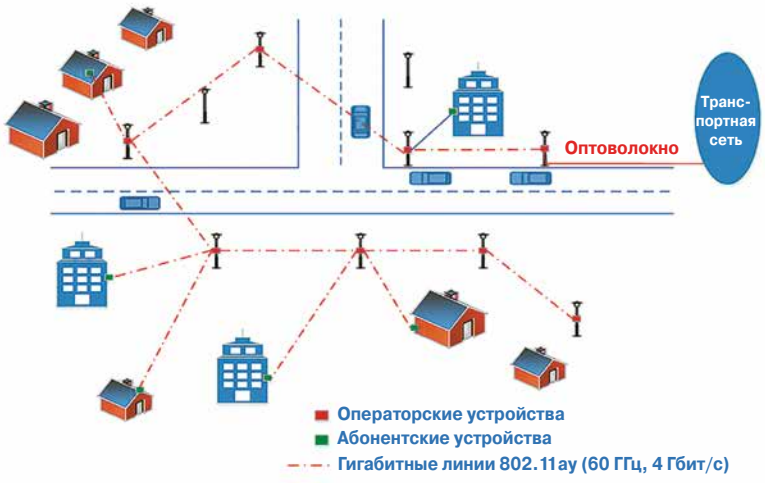


Рис. 2. Предоставление услуг фиксированного доступа в миллиметровом диапазоне средствами мультихоповой mesh-сети 802.11ay на скоростях до 4 Гбит/с ▼

Источники: 451 Research и Altiostar

◀ Рис. 3. Эволюция сотовой связи: от голоса – к всеобъемлющей сети, основанной на открытых стандартах

мого оборудования. Несколько особняком стоит уже упомянутая Huawei: одной из первых предложив миру операторские решения для сетей 5G, сегодня она занимает выжидательную позицию, так и не присоединившись пока ни к одному из альянсов, продвигающих открытые стандарты. Возможно, готовится к патентным войнам?

Реалии

В нашей стране внедрение сетей 5G пока буксует. Выделены несколько опытных зон, медленно и осторожно решается вопрос с выделением частот. Ясно, пожалуй, одно: российские сети 5G будут строиться на российском оборудовании и ПО – или при максимально доступной и возможной их локализации. Предприятия «Ростеха» сосредоточились, видимо, на радиооборудовании.

Один из интересных российских кейсов, основанных на принципах OpenRAN, – проект томской компании «Микран», который предполагает разработку радиомодулей сотовой связи 5G, включающих аппаратную платформу (аналоговый блок, цифровой блок и др.) и программное обеспечение цифрового формирования лучей и цифровой обработки сигналов на базе ПЛИС. Для работы на сетях связи с оборудованием других производителей будет обеспечена поддержка протокола O-RAN v2.0 и выше по интерфейсу eCPRI. В сообщении компании отмечается, что характерной особенностью ее проекта является разработка собственных элементов аналогового тракта – усилителей мощности и малошумящих усилителей для радиомодуля частотного диапазона 4,4–5,0 ГГц на основе полупроводников группы A_3B_5 собственной разработки.

В российскую рабочую группу OpenRAN входят специалисты Центра компетенций Национальной технологической инициативы «Технологии беспроводной связи и интернета вещей» при Сколтехе и эксперты МТС, «МегаФона», «Ростелекома» и «Вымпелкома». С рабочей группой сотрудничают ведущие российские разработчики и производители телеком-оборудования: «Элтекс» (Новосибирск), «Радио Гигабит» (Нижний Новгород), уже упомянутый «Микран» и др. Некоторые из них выпускают решения мирового уровня, давно и успешно работают на зарубежных рынках. Поставлены достаточно жесткие сроки – к концу июня 2020 г. необходимо финализировать план организации производства и внедрения отечественного оборудования, а до конца 2024 г. – запустить сети связи 5G в 10 городах России с населением более 1 млн человек. Несмотря на это, Сколтех как головная организация настаивает на том, чтобы план был скорректирован, поскольку рынок будет развиваться быстрее и важно, чтобы решение имело не только перспективы на российском рынке, но и потенциал экспорта в другие страны.

Следует отметить и нарастающий интерес промышленных предприятий к развертыванию собственных сетей 5G: в январе текущего года компании МТС, Ericsson и КАМАЗ сообщили о вводе в эксплуатацию первой промышленной сети 5G. Автопроизводитель рассчитывает, что сеть будет полезна при развертывании цифрового производства и разработке беспилотной автотехники. С учетом потенциала глубокой интеграции решений 5G OpenRAN в уже существующие корпоративные сети такая практика, возможно, будет востребована и другими предприятиями, активно внедряющими цифровые технологии.

Мобильные сети становятся сегодня важнейшим элементом критической инфраструктуры связи. Предстоит заметное переформатирование как интернета, так и сетей передачи данных в целом (рис. 3). Рынок будет измеряться десятками и сотнями миллиардов долларов. На кону – многое. ИКС

OpenRAN: теперь и в России

Системы, создаваемые в рамках проекта OpenRAN, смогут на равных конкурировать с лучшими иностранными решениями, считает главный конструктор ЛИЦ на базе Сколтеха по технологиям 5G Серафим Новичков.

В конце декабря 2019 г. Сколковский институт науки и технологий стал одним из победителей конкурсного отбора лидирующих исследовательских центров (ЛИЦ) в рамках нацпрограммы «Цифровая экономика РФ». ЛИЦ будет заниматься разработкой единого цифрового платформенного решения, обеспечивающего эффективное проектирование и развертывание сетей радиодоступа, на основе гармонизированного с международным открытого стандарта связи нового поколения (OpenRAN). Платформа будет включать специализированное ПО для базовых станций 5G и опытные образцы оборудования для сетей радиодоступа (RAN) 5G. Как ожидается, реализация проекта поможет создать в России собственный рынок оборудования для высокоскоростных беспроводных сетей, защищенный от внешних санкций и иных факторов риска. Заказчиком платформы выступает Министерство цифрового развития, связи и массовых коммуникаций РФ. Объем финансирования проекта, рассчитанного на три года, – 300 млн руб.

– Серафим, какие проблемы являются ключевыми для развития проекта и как планируется их преодолеть?

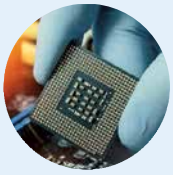
– Главная сложность – отсутствие в России достаточного количества квалифицированных кадров, в первую очередь специалистов с опытом разработки телеком-оборудования операторского класса. Это и программисты-алгоритмисты, и специалисты по встраиваемому ПО, и схемотехники, и эксперты по испытаниям телеком-оборудования. В России, несомненно, есть первоклассные программисты, однако для реализации проекта нужно иметь опыт создания и тестирования ПО и аппаратных решений для аналогичного по сложности радиооборудования и сетей связи общего пользования.

В Сколтехе мы собрали отличную команду, но не собираемся останавливаться на достигнутом и продолжаем ее усиливать. Поскольку Сколтех имеет статус международного университета, мы ищем кадры не только в России, но и за рубежом. С этого года расширяем набор студентов на образовательный трек, посвященный разработке для технологий IoT, 5G и будущих стандартов беспроводной связи: будем растить собственных специалистов.

– Почему основой создаваемой платформы выбрана именно концепция OpenRAN?

– Технологии OpenRAN выгодны и операторам, и регуляторам рынка. Они создают условия для более прозрачного и равноправного участия разработчиков в создании ключевой инфраструктуры, к которой, несомненно, относятся сети 5G. В ЕС, США, Великобритании и Китае сети 5G официально признаны основным драйвером экономики.

Важным преимуществом является и то, что в архитектуре OpenRAN разработчик не обязан создавать всю базовую станцию целиком. Он может сосредоточиться на разработке отдельных элементов сети радиодоступа, а значит, объем финансовых и человеческих ресурсов, необходимых для реализации такого проекта, заметно сокращается. И этот подход, как мы ожидаем, позволит нам на равных конкурировать с лучшими иностранными решениями.



В Воронеже создают новые транзисторы для сетей 5G

Инженеры воронежского Научно-исследовательского института электронной техники изготовили транзисторы для систем связи пятого поколения, обладающие улучшенными СВЧ-характеристиками.

Мощные СВЧ-транзисторы разработаны на многообещающем перспективном материале – полупроводниковом нитриде галлия. За семь лет работы в сотрудничестве как с отечественными, так и с зарубежными технологическими центрами специалисты НИИЭТ добились создания высокоэффективных транзисторных структур и изготовили на их основе серию сверхвысокочастотных транзисторов для нижнего диапазона частот сетей 5G (4–5 ГГц).

Мировой опыт разработки компонентов микроэлектроники на основе гетероструктур нитрида

– Будут ли разрабатываемые решения конкурентоспособны на мировом рынке?

– В противном случае этот проект просто не имеет смысла. Мы нацелены на создание решений, имеющих большой экспортный потенциал, так как внедрение сетей 5-го и следующих поколений (здесь мы скорее говорим о дальнейших релизах 5G, чем о полноценном поколении 6G, до которого минимум 10 лет) пока находится на раннем этапе. Поэтому сегодня самое время заниматься такими проектами.

Наше важное нетехнологическое преимущество в том, что это программное обеспечение никак не будет связано с американскими, европейскими или китайскими спецслужбами, а такой связи многие государства обоснованно опасаются.

– Когда можно ожидать появления первых опытных зон OpenRAN на оборудовании российских производителей?

– Согласно нашей дорожной карте, первые экспериментальные образцы мы получим в первом квартале 2021 г. Ближе к концу 2021 г. начнем испытания и предварительные демонстрации в опытной зоне 5G на территории Инновационного центра «Сколково».

– Какие платформы вы считаете наиболее подходящими для OpenRAN?

– Сегодня во всем мире популярна связка OpenRAN + COTS CPU (Commercial Off-The-Shelf CPU – готовые к использованию ЦП, например платформы x86). Также, на наш взгляд, пригодны для создания оборудования OpenRAN решения, предлагаемые компаниями Marvel, NXP, Xilinx.

– Планируете ли вы задействовать в своих разработках российскую элементную базу (ЭКБ)?

– Одно из преимуществ современных технологий, таких как различные виды виртуализации, NFV/SDN и пр., заключается в том, что они «отвязывают» специализированное ПО для телекомоборудования, скажем, ПО стека протоколов базовой станции, от конкретного аппаратного обеспечения, предоставляя возможность работать практически на любом «железе» с небольшой адаптацией. А это, в свою очередь, позволяет применять отечественную ЭКБ в современных телекоммуникационных сетях операторского класса.

Мы понимаем и разделяем опасения, связанные с использованием иностранной элементной базы, и готовы рассматривать все варианты взаимодействия с российскими производителями микроэлектроники. Так, ЛИЦ заключил соглашение с ГК «Элемент» о том, что мы совместно оценим возможность применения отечественной ЭКБ в наших разработках. У российских компаний («Байкал Электроникс», НПЦ «Элвис», ГК «Элемент», «Микрон») уже есть интересные наработки по процессорам. Мы верим, что выбор российских компонентов будет увеличиваться.

– С какими еще российскими компаниями вы сотрудничаете в проекте OpenRAN?

– Основные индустриальные партнеры ЛИЦ – «Элтекс» и «Радио Гигабит». «Элтекс» как крупнейший в России вендор телекоммуникационного оборудования (преимущественно транспортного уровня) будет отвечать за разработку аппаратного обеспечения модулей базовой станции, а также за дальнейшую передачу всего решения на производство. Компания «Радио Гигабит» отвечает за разработку ПО стека протоколов базовой станции физического уровня (L1-PHY).

– Считаете ли возможным выделение диапазона 700 МГц для обеспечения более широкого покрытия сетей LTE и 5G?

– Да, считаем, причем не только возможным, но и необходимым. Диапазон ниже 1 ГГц позволит создать «ковровое» покрытие, что для России с ее территориями очень важно. Также эти частоты выгодны для многих сценариев внедрения интернета вещей, что в итоге даст дополнительный экономический эффект. Сложно предсказать, когда произойдет перераспределение частот. Мы надеемся, что будет принято волевое решение и регулятор начнет выделять частоты для 5G, как это делают, например, в США и Китае. Кстати, именно нижний диапазон регуляторы ряда стран выделили для первого этапа развертывания 5G.

Беседовал Георгий Башилов

галлия с высокой подвижностью электронов показал преимущества этого материала, который может заменить и уже активно заменяет обычный кремний и арсенид галлия благодаря большей удельной выходной мощности на высоких рабочих частотах. До сих пор массовому применению данного материала препятствовали его высокая стоимость и несовершенство.

Теперь инженеры и технологи смогли повысить качество гетероструктур нитрида галлия почти до бездефектного уровня и изготовить на его основе устройства, работающие на частотах до 10 ГГц и выше с максимальной выходной мощностью в сотни ватт для оптимального применения в сетях 5G.

В НИИЭТ также ведутся работы по созданию силовых приборов на нитриде галлия для комплектования источников питания с повышенным КПД и меньшими габаритами, которые планируется внедрять при построении аппаратуры для сетей 5G.

Российские сети LPWA набирают абонентов

Виталий Мосеев

Число абонентских устройств, подключенных к LPWAN, в России пока не достигло 2 млн. Но развитие рынка подстегивают государственные инициативы, такие как обязательное оснащение новостроек умными счетчиками, а сети LPWA готовы не только к конкуренции, но и к эффективному взаимодействию.

LPWAN в мире…

В 2018 г. аналитики Berg Insight оценили количество устройств, подключенных к LPWAN (Low-power Wide-area Network; маломощные сети с дальним радиусом действия), в 1 млрд. Объем глобального рынка LPWA-сетей до 2024 г., согласно исследованию Market Study Report, будет прирастать ежегодно в среднем на 48,3% и к этому времени достигнет $3 млрд (в 2019 г. – $635 млн). При этом рынок сегментирован на сети лицензируемые и нелицензируемые (иначе говоря, на сотовые и несотовые). Лицензируемые сети LPWA (NB-IoT и LTE-M), по информации отраслевой ассоциации GSMA, на сентябрь 2019 г. работали в 57 странах мира.

Одна из крупнейших технологий нелицензируемых сетей, LoRaWAN, по данным LoRa Alliance, на конец 2019 г. охватывала 147 стран. Сеть Sigfox, основной конкурент LoRaWAN на глобальном рынке нелицензируемых сетей, представлена более чем в 70 странах с населением свыше 1,1 млрд жителей.

На рынке лицензируемых LPWAN конкуренция пока еще не слишком остра. Сети NB-IoT и LTE-M прошли стандартизацию 3GPP-консорциума (разрабатывает и принимает спецификации сотовой связи) в июне 2016 г. Среди преимуществ NB-IoT – поддержка более 100 тыс. устройств на соту, возможность работы устройства без подзарядки аккумулятора в течение десяти лет и более, охват одной базовой станцией объектов в радиусе нескольких километров (в зависимости от условий местности и плотности застройки). Экономия энергии достигается за счет более низких скоростей передачи и объемов данных. Например, одному счетчику в такой сети достаточно передавать в месяц объем данных до 1 Мбайт. Сеть NB-IoT позволяет управлять оборудованием с двухсторонней связью. В таких устройствах часто используется расписание активности.

Почти аналогичные характеристики имеют сети LTE-M. Однако для устройств в такой сети нужна большая полоса пропускания, а скорости передачи (1–4 Мбит/с) намного больше, чем у NB-IoT (26 кбит/с).

Примечательно, что с момента выхода стандартов потребовалось почти два года для того, чтобы оборудование стало массовым. Сети NB-IoT, как и LTE-M, строятся на базе существующей инфраструктуры 4G. Поэтому создавать такие сети могут только операторы с лицензией. Чтобы развернуть корпоративную сеть на основе NB-IoT или LTE-M, предприятию надо получать специальные лицензии. Высокая стоимость устройств NB-IoT (в сравнении с LoRaWAN) на старте не позволяла быстро привлекать заказчиков, но сейчас цены на модули NB-IoT снижаются.

LoRa – это запатентованное частотное расширение частотного спектра, разработанное французской фирмой Cycleo. Первые сети LoRaWAN запущены в 2015 г. Дальнобойность сети позволяет на открытом пространстве охватывать сигналом объекты, находящиеся на расстоянии 10–15 км, и до 5 км в условиях плотной городской застройки. Для работы устройствам не нужны SIM-карты. Из этого вытекает главное преимущество: сеть LoRaWAN может развернуть любое предприятие для собственных нужд. Для экономии энергии оборудование LoRaWAN работает по принципу асинхронной передачи: устройства «просыпаются» только тогда, когда им есть что передать. Для устройств, которым нужна двусторонняя связь, можно создать расписание активности.

Сети SigFox по охвату территории и автономности устройств во многом схожи с LoRaWAN. Различия в характеристиках в основном касаются полосы пропускания (нужны очень узкие фрагменты спектра), уровня собственного шума приемников (у LoRaWAN он больше) и реализации двусторонней связи (в SigFox такой функционал заложен по умолчанию).

…и в России

Среди сетей LPWA в России распространены как сотовые NB-IoT (разрешения на строительство таких сетей в стране выданы ГКРЧ мобильным операторам в январе 2018 г.; сейчас сети активно строятся и запускаются первые проекты), так и несотовые. В числе последних – LoRaWAN, сети локальных операторов: XNB (протокол компании «Стриж») и NB-FI (протокол компании Waviot), а с марта 2020 г. и SigFox. Эти сети также не требуют лицензирования, а устройства могут работать до десяти лет без подзарядки. Конкретные преимущества, как правило, указывают сами владельцы локальных протоколов.

Сети SigFox в России до недавних пор не были официально представлены. Но в начале 2020 г. была создана компания Sigfox Russia, эксклюзивный дистрибьютор Sigfox в России, а в марте – объявлено о ее партнерстве* с венчурной компанией Energo Capital (работает в России и странах Балтии). Стороны намерены совместно развивать в России сеть интернета вещей 0G (уже работает в Латвии и Литве), в среднесрочных планах 0G – строительство сети в Сибири, а также в районе Северного морского пути – с применением спутниковой связи ELO от Eutelsat.

В России, по оценкам Андрея Колесникова, директора Ассоциации интернета вещей, насчиты-

* См. https://iotdaily.ru/2020/03/13/set-sigfox-prihodit-v-rossiyu.

вается не более 2 млн абонентских устройств в сетях LPWA и не более 100 тыс. таких базовых станций. Сегмент LPWAN займет всего 5% рынка IoT в 2021 г. (без учета операторского NB-IoT).

Регулирование помогает росту

Развитию рынка в краткосрочной перспективе могут способствовать несколько факторов. Среди них эксперты выделяют отсутствие чрезмерного регулирования области интернета вещей со стороны государства, объединение игроков рынка IoT в профессиональные сообщества и рабочие группы совместно с госорганами.

К примеру, отраслевое российское законодательство отчасти позволит вырасти рынку, полагает Павел Захаров, директор по маркетингу корпоративного бизнеса «Мегафона». Согласно поправкам в Федеральный закон «Об электроэнергетике», напоминает эксперт, с 1 июня 2020 г. все новые многоквартирные дома должны быть оснащены «умными» приборами учета электроэнергии, а с 1 января 2023-го все без исключения счетчики учета электроэнергии должны быть заменены на автоматизированные решения. «Таким образом, в ближайшие три года емкость рынка LPWAN может вырасти до 20 млн новых подключений», – подсчитывает П. Захаров.

В Дорожной карте развития «сквозной» цифровой технологии «Технологии беспроводной связи»*, утвержденной в октябре 2019 г., решения LPWAN признаны вторыми по значимости после 5G. На развитие технологий LPWAN будут выделяться средства в рамках национального проекта «Цифровая экономика РФ», говорит Владимир Шапоров, руководитель направления Центра развития телекоммуникационных решений компании «Техносерв». Разработка ПО и оборудования для технологий LPWAN, в том числе NB-IoT, отмечает эксперт, включена в Дорожную карту развития СЦТ «Технологии беспроводной связи» в России до 2024 г.

Тенденции ближайшего будущего

Среди текущих тенденций рынка – наращивание функционала LPWAN и появление новых сценариев их применения.

Сбор данных для оптимизации процессов

Участники рынка ищут возможности монетизации собираемых в LPWAN данных. Например, обезличенные данные абонентов сотовой связи о местонахождении стали основой для рынка геоаналитики. Нечто подобное появится и в LPWAN, главное здесь – нарастить число проектов с большим количеством устройств.

«Стали появляться компании, переходящие от пилотных проектов в 10–30 датчиков к коммерческим поэтапным проектам, в которых реализуется от 1000 и более датчиков, – говорит Виктор Мазурик, директор по маркетингу и монетизации инноваций компании «ЭР-Телеком холдинг». – В 2020 г. проекты начнут двигаться от функций простого мониторинга и диспетчеризации к управлению и предиктивному обслуживанию». Возможно, агрегация данных с LPWAN-устройств и анализ информации позволят предприятиям оптимизировать бизнес-процессы.

LPWAN на полях

Сети LPWA используются в сельском хозяйстве для контроля характеристик почв. На одном и том же участке поля структура почвы может различаться по химическому составу, температуре и влажности, для мониторинга этих параметров в почву устанавливаются специальные датчики. Агрономы, к примеру, знают, что в точке А влажность достаточна, а в точке Б – избыточна, и исходя из этого, принимают решение об оптимизации расхода воды на точку Б. Точно так же оптимизируется расход удобрений. Когда урожай собран,

* См. https://digital.gov.ru/ru/documents/6674.

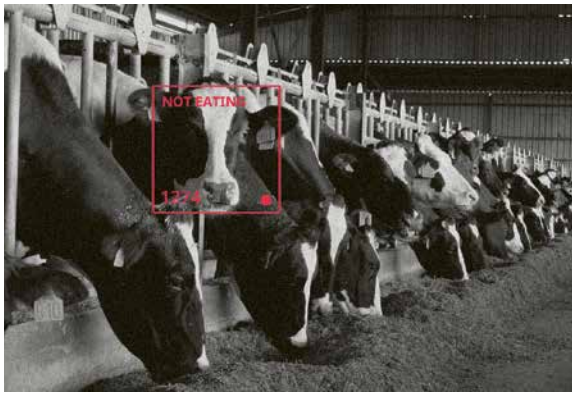
Рынок интернета вещей в России

По данным Ассоциации интернета вещей, консолидированный рынок IoT в России в 2019 г. вырос на 9% по сравнению с 2018 г. Ожидалось, что темпы прироста будут несколько выше (+15%). Как отмечает Владимир Шапоров из компании «Техносерв», объем рынка в 2020 г. может превысить 80 млрд руб. (оценка взята из исследования Schneider Electric и ЦСП «Платформа»). В 2020 г. темпы роста IoT-рынка останутся на прежнем уровне (это 8–9%), полагает Павел Захаров из «Мегафона». По его словам, интернет вещей – это второй по величине сегмент клиентов после голосовых пользователей. В России в различных устройствах, подключенных к интернету, используется более 20 млн SIM-карт. Однако операторский интернет вещей сейчас представлен в основном сетями 2G/3G/4G, а не LPWAN.

По мнению Виктора Мазурика из «ЭР-Телеком холдинг», лидерство нелицензируемых LPWAN объясняется неразвитостью сетей NB-IoT. «Во-первых, строительство сетей в лицензируемых диапазонах (NB-IoT) началось лишь в середине прошлого года. Поэтому фактически сети просто не успели развернуть. Во-вторых, ассортимент оборудования для таких сетей довольно мал, тогда как для нелицензируемых он расширяется заметными темпами», – поясняет В. Мазурик. Например, количество новых устройств для LoRaWAN выросло в 2–2,5 раза.

датчики LPWAN используются на складах, помогая предотвратить распространение гнили.

Постепенно технология захватывает новые сегменты. Например, компания МТС рассматривает возможность использования LPWAN для своего решения «Умная ферма». Входящий в него умный датчик-болюс проглатывает корова, устройство постоянно находится в же-



лудке животного, не причиняя ему дискомфорта. Данные с датчика помогают персоналу контролировать показатели физической активности, потребление воды, корма, снизить количество медикаментов на 15% и предугадывать отел за 15 часов.

Контроль в промышленных масштабах

LPWAN-решения помогают контролировать заполненность резервуаров с химикатами на производствах. При недостатке реагентов автоматически рассылаются оповещения о необходимости пополнить их запас. Таким образом, производство не простаивает, а службы, отвечающие за закупки, действуют оперативнее.

Оптимизируются и затраты на воду, газ и электроэнергию. Для этого применяются счетчики и датчики утечек, которыми оснащают трубопроводы. Информация о расходе ресурсов автоматически и с заданным интервалом отправляется диспетчерам. Такая схема пришла в промышленность из ЖКХ, где LPWAN-оборудование используется достаточно давно.

Нелицензируемые сети в глуши

Развитие сетей на базе LoRaWAN/NB-Fi/XNB в нелицензируемых диапазонах будет идти не только в городах, но даже там, где нет мобильной связи. Зачастую это единственный и альтернативный спутниковому канал связи. Развертывать такие сети легко и недорого, а желание сэкономить на счетах за связь есть у многих предприятий. «Круг владельцев сетей LoRaWAN может пополниться крупными корпоративными игроками нефтегазового сектора, нефтехимии, металлургии и других сфер, перед которыми будет стоять задача обеспечить предприятия связью для IIoT-решений, в том числе в труднодоступной местности», – полагает В. Шапоров.

Умные города с LPWAN

Сети LPWA пригодятся и для реализации концепции умного города. Датчики отслеживают загруженность парковок и через мобильное приложение могут оповещать водителей о свободных местах поблизости. С помощью датчиков LPWAN, контролирующих наличие вредных примесей в воздухе, можно построить интерактивные карты экомониторинга, и в некоторых городах мира они доступны населению. К примеру, жители мегаполисов с их помощью выбирают оптимальные маршруты для прогулок с детьми. Помогут сети дальнего радиуса действия и в уборке мусора: для этого LPWAN-датчики прикрепляют к мусорным бакам. Сенсоры сообщат диспетчерам коммунальных компаний о заполненных баках и необходимости их очистки.

Сети NB-IoT заменят GSM

Операторы мобильной связи, развертывающие лицензируемые сети LPWA, не исключают перехода на новые технологии. Скорее всего, на замену GSM придут NB-IoT. Главным драйвером роста технологии станет удешевление оборудования и появление датчиков для различных сценариев. «В 2019 г. стоимость чипа NB-IoT упала до $5–6. Но датчики и модули стандарта GSM все еще обходятся конечному потребителю дешевле, поэтому пока датчики NB-IoT не смогут заменить GSM-устройства. С другой стороны, в США, Японии и некоторых других странах сети GSM уже прекратили работу, поэтому глобальный рынок интернета вещей начал постепенный переход на стандарты NB-IoT и LTE-M», – поясняет П. Захаров.

Эффективное сочетание технологий

В 2019 г. сотовые операторы России объявили о начале развертывания сетей NB-IoT. Небольшие пилотные проекты были запущены в ряде городов. К сожалению, после утверждения стандарта NB-IoT эффективных устройств долгое время не было. Теперь дефицит уходит в прошлое, а стоимость чипов имеет многолетнюю тенденцию к падению, что способствует доступности NB-IoT. «В 2020–2021 гг. зона действия сетей на базе NB-IoT, вероятно, будет расширена до полного соответствия покрытию на федеральном уровне», – считает В. Шапоров. В итоге у клиентов, отмечает В. Мазурик, появится возможность реализовать более сложные проекты, сочетая NB-IoT с другими LPWAN-технологиями.

Развитие LPWAN, соглашаются эксперты, в ближайшей перспективе будет происходить органично. По их консолидированному мнению, разные сети LPWA имеют разные особенности, поэтому могут эффективно взаимодействовать и дополнять друг друга, позволяя комбинировать выполнение сценариев и задач. ИКС

RPA: ступень к цифровизации

Технология роботизированной автоматизации бизнес-процессов достигла того уровня развития, когда предприятия могут ее внедрять, не тратя время на пилотирование, и получить ощутимую выгоду без значительных вложений.

Игорь Новиков, независимый эксперт

Технологию RPA (Robotic Process Automation), которая сегодня находит все более широкое применение, можно рассматривать в качестве промежуточной ступени к «большой» цифровизации. Эта технология представляет собой набор скриптов (сценариев) или программных ботов, выполняющих в бизнес-процессах те же операции, которые раньше выполнял человек, но с большей производительностью. RPA-боты функционируют поверх программных приложений. Они считывают с экрана или из вычислительной системы данные, необходимые для следующего действия. Выбор очередной бизнес-команды осуществляется в автоматическом режиме.

Действуя по такой схеме, RPA-бот может запускать обработку данных, передавать информацию из одного приложения в другое. Бот способен оценить возникшую ситуацию, применяя доступные ему «сенсорные технологии», и обеспечить ответную реакцию со стороны прикладной системы в зависимости от сделанного им выбора. Под «сенсорными» понимаются технологии автоматизации сбора исходных данных и их первичной оценки, заключающиеся в замене человека на некий «сенсор». Это может быть чтение новостей на том или ином веб-сайте или создание сканов экрана с последующей оценкой обнаруженных данных. «Сенсор» может ожидать появления определенного сообщения по электронной почте, чтобы в зависимости от его «смысла» выбрать дальнейшие действия.

Однако это не искусственный интеллект. Мы называем такую систему RPA-ботом (или RPA-роботом), подчеркивая, что она выполняет только те действия, которые были заложены в план ее работы прикладным программистом. RPA-бот выполняет те же действия, что и человек, но изменить свой выбор, как человек, не может – он выбирает ту команду, которая доступна ему среди заранее подготовленных вариантов, не используя технологии ИИ и машинного обучения.

Прежде всего, RPA поднимает производительность обслуживаемой программной системы: прежний набор операций теперь выполняется с более высокой скоростью. Попутно исключаются ошибки, которые раньше мог допустить человек. Вместе с тем уже на старте своего внедрения RPA позволяет добиться взаимной координации работы нескольких приложений. Более того, RPA позволяет быстро осуществить интеграцию работы нескольких прикладных систем, не сравнимую по затратам с альтернативными способами (на уровне интерфейсов, данных, веб-сервисов и пр.). В результате расходы на обслуживание ИТ-систем снижаются.

«Пришелец» из 1950-х

Принято считать, что инструменты для нынешней роботизации являются порождением недавнего времени. Однако RPA имеет более давнюю историю.

Одним из пионеров этой технологии называют исследователя из компании IBM Артура Самуэля. В 1959 г., работая над прообразом системы искусственного интеллекта и машинного обучения, он сформулировал базовые принципы, которые в дальнейшем легли в основу RPA.

Артур Самуэль работает со своей программой Checkers

Суть его идеи состояла в том, что для роботизации нужно не стремиться запрограммировать все возможные сценарии, а научить компьютеры самообучаться. В результате была создана компьютерная программа Checkers («Игровые шашки»), ставшая одним из первых в мире примеров самообучающейся программы-робота.

Исследования в области самообучающихся роботизированных систем стимулировали работы в других направлениях, необходимых для новой технологии: решении задач на естественном языке; трансляции заданий из одной предметной области в другую; извлечении смысла из текстовых данных. Изучение компьютерного интерфейса и применение средств формализации для его оценки привели к развитию обработки команд на естественном языке (Natural Language Processing, NLP). Благодаря этой технологии программы научились понимать и обрабатывать обычный текст, созданный человеком. И хотя до умения читать между строк и понимать сленг еще далеко, эти разработки помогли прийти к созданию технологии RPA. Однако ее становление затянулось на десятилетия.

Во второй половине 1990-х гг. была разработана технология автоматического чтения контента с экрана дисплеев (скрапинг, scraping), что имело большое значение для RPA. Благодаря скрапингу программы научились извлекать данные из различных источников: страниц вебсайтов, программ, документов. Если раньше чтение осуществлялось вручную и требовало существенных затрат времени на осмысление собранных данных, то скрапинг перевел процесс на рельсы автоматизации. Уже к началу 2000-х гг. эта технология достигла уровня, допускающего ее практическое применение. Скрапинг стал фундаментом для первых, пока простых RPA-инструментов.

Появились первые внедрения RPA, но рынок развивался вяло. Многие RPA-продукты оставались неизвестными рынку. Рост сдерживался тем, что внедрение RPA требовало значительных затрат на подготовку, поэтому такие продукты могли эффективно применяться только для задач, связанных с неизменными, повторяющимися последовательностями команд. Рынок ждал перехода на следующее поколение RPA, обладающее функцией упрощенной оценки собираемого контента, на основе которой принимается решение о дальнейшей работе робота. Такие продукты стали называть когнитивными или «умными» RPA (cognitive, intelligent RPA).

Мейнстримом RPA стала с 2015 г. Этому способствовало также развитие систем оптического распознавания символов (OCR), применение NLP и машинного обучения для обработки данных сложной структуры (частично структурированных и хаотично расположенных). В результате появилась технология RPA в том виде, какой мы знаем ее сегодня.

RPA на старте 2020 г.

По оценкам Deloitte Insights, 2019 г. стал переломным для роста популярности RPA. Если еще два года назад эту технологию рассматривали как «кладезь неиссякаемых возможностей для будущего развития, но еще слишком разрозненных для внедрения», то теперь за RPA признали «огромный подтвержденный потенциал для бизнеса и общества».

Большое значение для восхождения RPA на рынке имело исследование Magic Quadrant for RPA Software 2019, опубликованное Gartner летом прошлого года. В нем аналитики предсказали, что к концу 2019 г. мировой рынок роботизированной автоматизации достигнет $1,3 млрд. Их оптимизм основывался на результатах 2018 г., когда рост составил 63,1%. Экспертов Gartner поддержали и другие аналитические компании. В McKinsey & Co заявили, что рассчитывают увидеть к 2025 г. подъем всего рынка средств автоматизации до уровня $6,7 трлн, называя RPA главным двигателем подъема этого направления в мире.

В то же время эксперты выделили два серьезных препятствия на пути RPA. Первое – все еще недостаточно высокое качество собираемых данных, которые используются для работы RPA-механизмов. Многие специалисты возлагают большие надежды на развитие технологий маркировки данных. Они должны помочь повысить качество обучения ИИ и привести к появлению моделей данных, гарантирующих нужный для RPA-расчетов уровень доверия к ним.

Второй «камень» на пути RPA – это пестрый «винегрет» из прежних проектов роботизации. Многие компании в мире благодаря им уже прошли первый, упрощенный этап автоматизации. Теперь им предстоит внедрять новые, более совершенные RPA-системы, что заставит обратить серьезное внимание на предварительную оценку и планирование.

Ведущие мировые RPA-платформы

В упомянутом выше магическом квадранте Gartner отнесла к лидерам рынка RPA три компании – Automation Anywhere, Blue Prism и UiPath.

Automation Anywhere

Разработку этой RPA-системы начала в 2003 г. американская компания Tethys Solutions, которая в 2010 г. переименовалась в Automation Anywhere по названию своего ос-

новного продукта. Система известна в первую очередь ярким набором крупных заказчиков – AT&T, Dell, General Motors, Google, LinkedIn, Tesco, Whirlpool, Wipro и др. Эта база помогла привлечь значительные средства в развитие системы. В 2018 г. были получены крупные инвестиции от New Enterprise Associates, Goldman Sachs и SoftBank.

Результат не заставил себя ждать. Сегодня Automation Anywhere – глубоко модернизированный RPA-продукт, предлагающий не только традиционный механизм RPA, но и такие новшества, как поддержка неструктированных данных и применение смарт-элементов NLP. Структурно Automation Anywhere представляет собой набор продуктов: аналитическая платформа Bot Insight для получения оперативной и бизнес-аналитики в реальном времени; платформа Bot Farm корпоративного уровня для запуска ботов по требованию; «магазин ботов» Bot Store с уже готовыми сценариями для бизнес-автоматизации; мобильное приложение RPA. К этой базовой инфраструктуре заказчик затем приобретает массив компонентов, которые могут обмениваться между собой данными, помогая компании выстраивать гибкие сценарии автоматизации.

Blue Prism

Британская компания Blue Prism Group появилась в 2001 г. и была одной из первых, кто осознал большие перспективы прикладных средств автоматизации бизнес-задач на рынке программных услуг для предприятий. Ее первый коммерческий RPA-продукт Automate был выпущен в 2003 г., два года спустя он был модернизирован и мог широко масштабироваться в рамках предприятия.

Интеллектуальная RPA-платформа Automate состоит из трех основных элементов. Object Studio позволяет создавать блочным методом программные процедуры для автоматизации бизнес-процессов; логика обработки задается через систему триггеров. Второй элемент – Digital Workforce – набор автономных программных роботов, обладающих некоторыми элементами ИИ. Наконец, третий элемент – Control Room – представляет собой механизм для управления процессами, запущенными на базе работающих роботов.

UiPath

RPA-платформу UiPath разработала группа предпринимателей из Бухареста в 2005 г. Сначала UiPath внедрялась в Румынии, затем территория присутствия постепенно расширялась, и вскоре были открыты офисы в Лондоне, Нью-Йорке, Бангалоре, Париже, Сингапуре, Вашингтоне и Токио. После выхода в 2017 г. на американский рынок и открытия штаб-квартиры в Нью-Йорке рост числа заказчиков резко ускорился. В 2019 г. их насчитывалось уже более 5 тыс.

UiPath интересна тем, что позволяет внедрять средства автоматизации как локально, так и путем автоматического развертывания в облаке. Продукт имеет активную поддержку со стороны значимых партнеров, широко используется для управления бизнес-процессами, анализа данных и применения средств ИИ.

UiPath представлена рядом базовых элементов. Платформа UiPath Platform служит для быстрой автоматизации однотипных, повторяющихся процессов; редактор UiPath Studio предназначен для программирования готовых компонентов автоматизации и построения рабочих процессов автоматизации; механизмы UiPath Robots позволяют реализовать заложенные операции, управление которыми ведется из централизованной панели UiPath Orchestrator.

RPA в России

Еще пять лет назад к автоматизации информационного обмена между бизнес-системами на российском рынке подходили исключительно с классических позиций: сначала внедрялись готовые продукты и выстраивались интеграционные связи с другими системами, если это предусмотрел разработчик решения. Однако индивидуальные особенности каждой компании часто требовали большего. В результате рутинные операции для поддержки взаимодействия между системами выполнялись сотрудниками вручную. Эволюция экосистемы откладывалась до следующего проекта и требовала крупных инвестиций.

Курс на цифровизацию способствовал росту популярности RPA в России. Внедрение этой технологии стало новым направлением бизнеса для крупных российских интеграторов: КРОК, «Инфосистемы Джет», Softline и др.

«Сегодня рынок RPA-решений хорошо наполнен, – рассказывает Станислав Маслов, руководитель направления роботизации и заказной разработки компании Softline. – В России успешно внедряются решения на платформах мировых лидеров, и существуют как минимум три российских продукта, которые практически в полной мере покрывают задачи роботизации процессов».

Теперь фактически каждый вендор готов предоставить многофункциональный продукт, состоящий из различных модулей, которые в совокупности не только обеспечивают полноценную автоматизацию бизнес-процессов (роботы и люди работают «рука об руку»), но и решают сопутствующие задачи, такие как интеллектуальное распознавание документов или Process Mining. Сегодня ни одна из ведущих платформ уже не позиционируется как RPA-решение в чистом ви-

де. «Создание полноценной экосистемы роботизации, включающей компоненты искусственного интеллекта и машинного обучения, – вот основной тренд на рынке», – добавляет С. Маслов.

ROBIN

Одна из первых российских RPA-разработок – платформа ROBIN – появилась на рынке в январе 2018 г. Система написана на C# и Java и предназначалась для внедрения в сегменте крупного и среднего бизнеса. Новый продукт отличают русскоязычные интерфейс и документация, а также доступность локальной техподдержки. Это большое преимущество для RPA-проектов, где важен не только набор внедряемых функциональных средств, но и глубокий учет особенностей существующей у заказчика ИТ-экосистемы. Для государственных структур немаловажным фактором является включение платформы ROBIN в реестр российского ПО.

К функциональным преимуществам ROBIN часто относят наличие встроенного классификатора неструктурированных текстов, отдельного инструмента для создания текстовых чатботов, поддержку различных вариантов интеграции с другими российскими бизнес-продуктами. В их число входят, например, ABBYY FlexiCapture и Yandex OCR, используемые для распознавания документов, а также Word, Excel, Outlook, почтовые сервисы, FTP/SFTP, Google Sheets, вызовы любых REST- и SOAP-сервисов. Исходные данные ROBIN получает через собственный API, который поддерживают ROBIN Agent и ROBIN Orchestrator.

Главным преимуществом ROBIN называют простоту создания роботов. Если пользователем большинства зарубежных платформ является прежде всего программист, то настройку программных роботов для ROBIN может выполнять бизнес-аналитик. Это позволяет быстрее внедрить платформу – на что требуется две-четыре недели – и значительно уменьшает себестоимость проекта.

ABBYY Vantage

Появление RPA-продукта от ABBYY было ожидаемым. На это указывал интерес, который компания проявляла к развитию систем на основе ИИ. В то же время до недавних пор ABBYY ограничивалась лицензированием имеющихся технологий распознавания для других разработчиков. Сегодня эти технологии у нее лицензируют топ-10 ключевых игроков рынка RPA, среди которых UiPath, WorkFusion, NICE Systems и Kyron Systems. ABBYY заключила также соглашения о стратегическом партнерстве с UiPath и Blue Prism, благодаря которым универсальная платформа для интеллектуальной обработки информации ABBYY FlexiCapture может быть интегрирована в продукты названных вендоров.

Недавно стало известно, что компания готовит к запуску новый RPA-продукт ABBYY Vantage (сегодня он уже запущен в США по программе раннего доступа). Разработчики относят ABBYY Vantage к RPA-платформе нового поколения, которая призвана стать основой для выстраивания экосистемы интеллектуальной обработки информации, наделяющей программных роботов когнитивными навыками. В число их умений входят чтение документов любой сложности, понимание смысла текста, извлечение ценных данных из документов любых типов, принятие решений, которые до сих пор могли принимать только люди. Так, новая платформа позволяет проверять комплектность документов или определять необходимость запроса дополнительной информации.

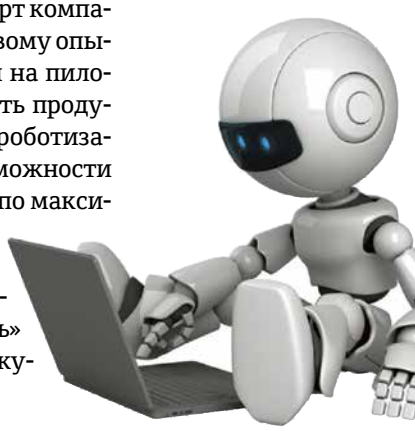
С технической стороны ABBYY Vantage представляет собой интеллектуальный конструктор, который может быть легко интегрирован в различные платформы бизнес-автоматизации, такие как RDA (Robotic Desktop Automation), DPA (Digital Process Automation) и т.д. Пользователь может выбрать необходимые навыки для любого программного робота, наращивая без сложных настроек их когнитивные навыки.

Пора действовать

Интеграторы сегодня хорошо понимают, что на рынке появились технологически продвинутые RPA-инструменты, и теперь основной задачей бизнес-автоматизации становится адаптация технологии и развитие умений для их практического применения.

«Раньше, когда технология RPA только появлялась в компаниях, – рассказывает С. Маслов, – выбирались программная платформа и самый рутинный процесс, после чего автоматизация начиналась. Сейчас мы пытаемся уйти от такой концепции и предлагаем клиентам сразу выстроить процедуру так, чтобы максимально быстро реагировать на запросы бизнеса. Мы уже неоднократно убеждались – технология работает, процессы для автоматизации есть, а выгода достигается без серьезных вложений».

В нынешней ситуации, считает эксперт компании Softline, «следует довериться мировому опыту и вместо того, чтобы тратить время на пилотирование и оценку результатов, начать продуманное, последовательное внедрение роботизации». Именно в таком случае все возможности современных платформ используются по максимуму, а сами платформы постоянно развиваются и обрастают новыми сервисами. Пора от экспериментов переходить к действиям, чтобы «не проспать» цифровую трансформацию своих конкурентов и не остаться позади. ИКС



COVID-19 и ЦОДы: минимизация рисков на критических объектах

Uptime Institute Intelligence team

Рекомендации экспертов Uptime Institute помогут операторам ЦОДов противостоять воздействию коронавируса, а также разработать стратегии и процедуры на случай эпидемических ситуаций в будущем.

Публикуется в сокращении.

В условиях пандемии критически важные объекты сталкиваются с особыми трудностями, как из-за возможного отсутствия ключевых сотрудников по причине болезни или карантина, так и в силу других факторов, которые могут повлиять на способность оператора поддерживать непрерывную работу объекта. К счастью, поддержание высокой готовности у отрасли ЦОДов записано в генах и проверено богатым опытом противостояния отключениям электропитания, пожарам, сложным погодным условиям и прочим потенциально опасным событиям. Применяемые в большинстве ЦОДов процедуры обеспечения непрерывности процессов могут быть адаптированы и к вызовам пандемии.

Подготовка бизнеса

В первую очередь необходимо разработать план готовности к пандемии. Если специального плана нет, можно использовать тот, что был подготовлен к другим ЧС. План должен включать многоуровневое реагирование, четко определять действия, которые необходимо предпринять на каждом уровне, и обстоятельства, ведущие к эскалации на следующий уровень. Большинство организаций имеют план действий в условиях ЧС из трех–пяти уровней – от принятия мер предосторожности до приостановки эксплуатации и в наихудших случаях – полного закрытия площадки с переводом критических приложений и операций на резервные площадки. В плане должны быть предусмотрены ситуации, когда персонал не сможет получить доступ на площадку или, напротив, должен покинуть ее в кратчайший срок.

Кроме того, следует оценить влияние пандемии на ИТ- (клиентские) сервисы. Реакция некоторых клиентов на COVID-19 может сказаться на объемах интернет-трафика, рабочих нагрузках и уровне доступности сервисов. Операторам рекомендуется обсудить с клиентами любые возможные воздействия на их работу, особенно при планируемых обновлениях или миграциях систем, наращивании мощностей, а также вероятные задержки намеченных проектов.

Важно поддерживать коммуникации с персоналом, клиентами и партнерами. В быстро меняющихся условиях совещания следует проводить часто: ежедневно или даже дважды в день. Необходимо оперативно информировать персонал о течении пандемии и лучших практиках поддержания безопасной и здоровой рабочей среды. Кроме того, следует дать персоналу четкие указания относительно поведения при проявлении симптомов заболевания (в том числе у членов семьи), порядка и продолжительности самостоятельного карантина, предоставления больничного, страхового покрытия и т.п.

Следует быть готовым к нарушениям в цепочке поставок. В дополнение к обеспечению основных ресурсов нужно наладить поставки продукции, препятствующей распространению инфекции: дезинфицирующих салфеток, средств для мытья рук, масок, перчаток, бесконтактных термометров и т.д. Также рассмотрите вероятность долгосрочного нарушения цепочки поставок критических запчастей. Компоненты, производимые в Китае или других регионах, сильно пострадавших от эпидемии, могут оказаться малодоступными в течение многих месяцев. (Обратите внимание, что ряд крупнейших заводов по производству оборудования отопления, вентиляции и кондиционирования (ОВК) располагаются в Италии).

Важно избегать ненужных рисков. Отложите или отмените проекты и мероприятия, которые могут увеличить риск заражения, повлечь за собой высокие затраты или повысить нагрузку на поставщиков, партнеров и персонал.

Защита площадки и персонала

В то время как многие шаги, которые необходимо предпринять, подразумевают участие партнеров, защита непосредственно площадки и персонала – первоочередная задача самого оператора ЦОДа.

Санитарная обработка

При вирусной пандемии санитарная обработка очень важна. Уровень защиты помогут повысить следующие шаги:

- Усиление уборки объекта: ежедневно проводите несколько циклов очистки, особенно поверхностей, на которые приходится большое число контактов (дверные ручки, выключатели освещения, кнопки лифта, поручни, водопроводные краны и т.п.).
- Размещение дезинфицирующего средства для рук и дезинфицирующих салфеток (а также бытовых мусоросборников) по всему объекту. Сделайте вывески с напоминанием персоналу и посетителям о необходимости их регулярного использования. Требуйте, чтобы персонал дезинфицировал все рабочие места в начале и в конце каждой смены.
- Использование для дезинфекции аэрозолей. Это более эффективно, чем протирание поверхностей дезинфицирующими растворами, поскольку распыляемый антисептик покрыва-

ет поверхности на более длительный период времени.

- Глубокая очистка пространства машзалов. Увеличьте частоту как стандартных действий по уборке (внешних поверхностей стоек с оборудованием и т.п.), так и глубокой уборки (полная очистка оборудования, уборка под фальшполом, за фальшпотолком, распыление дезинфицирующих составов и т.п.).
- Ограничение применения тамбур-шлюзов и/или их дезинфекционная обработка после каждого использования. Тамбур-шлюзы могут быть местом размножения вируса, поскольку являются малыми, изолированными, обычно непроветриваемыми пространствами и на их внутренних поверхностях вирусы могут жить в течение многих часов, если не дней.
- Пересмотр сроков плановой замены воздушных фильтров в системе ОВК. Заменяйте воздушные фильтры чаще и/или используйте более эффективные фильтры.
- Возможный наем специализированной уборочной компании, которая следует рекомендациям по дезинфекции, выпущенным регулирующими органами (в России – Роспотребнадзором).
- Возможное расширение круга специализированных компаний по уборке технологических помещений и машинных залов исходя из двух сценариев. Предупредительный сценарий: для уборки используются одобренные моющие средства и материалы, которые удаляются с объекта и утилизируются сразу по завершении уборки. Сценарий с подтвержденным заражением COVID-19 на объекте: уборщик использует костюм биологической защиты, перчатки, бахилы и средства; все они удаляются с объекта сразу по завершении уборки.

Ограничение доступа

Доступ на критический объект строго контролируется – что весьма полезно с точки зрения снижения риска инфицирования. Дополнительно рекомендуем:

- На КПП при входе на территорию ЦОДа осматривать проходящих, измерять температуру бесконтактными методами и дезинфицировать. Вход на площадку должен быть разрешен только в том случае, если состояние посетителя не вызывает сомнений.
- Придерживаться консервативного подхода: рассматривать любой подозрительный симптом как возможный случай инфекции COVID-19 (как правило, проведение оперативных тестов на COVID-19 на месте невозможно).
- Совместно с отделом кадров и/или отделом по охране труда разработать опросный лист для выявления заболевающих и обязать всех посетителей объекта (включая сотрудников) перед доступом на площадку заполнять этот лист.
- Установить информационные стойки по самооценке состояния здоровья у всех входов и в людных местах.

Организация работы персонала

Приведенные ниже рекомендации следует рассмотреть вместе с руководителями подразделений по управлению кадрами и обеспечению безопасности.

- Протестируйте все соединения VPN для обеспечения надежного доступа, затем переведите весь персонал, не отвечающий за критические процессы в ЦОДе, на надомную работу. Обеспечьте доступ через VPN к системе управления зданием для удаленного мониторинга ЦОДа. Дайте персоналу подробные инструкции по подключению через VPN.
- Обеспечьте доступ к стандартным и аварийным эксплуатационным процедурам для возможности удаленного управления в случае необходимости. Убедитесь в точности описания данных процедур, а также в том, что они могут быть корректно исполнены лицами, для которых это не входит в должностные обязанности.
- Задействуйте технологии удаленного мониторинга/управления (например, удаленные «умные» руки), автоматизации и т.д. Заранее проведите стресс-тестирование применяемых технологий и процедур.
- Отложите/отмените все личные встречи – используйте электронную почту, телефонную и аудио/видеоконференцсвязь.
- Будьте готовы к сложностям, вызванным снижением численности работающих. Разработайте матрицу угроз для различных сценариев невыхода сотрудников на работу (например, менее чем 25%, 25–50%, 50–75%, 75–99%). Для каждого сценария учитывайте влияние на бизнес (критические и некритические функции), эксплуатацию ЦОДа, уровень сервиса и т.д.
- Отправляйте на самоизоляцию и удаленную работу в течение следующих 14 дней сотрудников с симптомами заболевания. Сотрудникам, имевшим тесный контакт с подтвержденным носителем COVID-19, следует также уйти на карантин на 14 дней.
- Пересмотрите назначения критически важных сотрудников и их заместителей и убедитесь, что заместители полностью обучены и проинструктированы о ролях и обязанностях

критически важных сотрудников, которых им может потребоваться временно заменить.

Ограничение перемещений

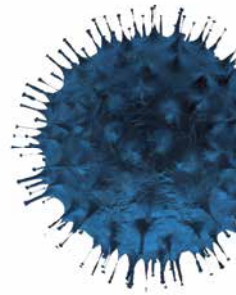
Во время вспышки эпидемии компании и органы власти вводят ограничения на перемещения. Соответствующие правила будут ужесточаться или смягчаться в зависимости от ситуации. Необходимо рассмотреть возможность введения следующих мер:

- Запретить поездки, не являющиеся неотложными (или сократить их число).
- Запретить перемещения между площадками (или сократить их число). Если такая поездка необходима, убедитесь, что вероятность перекрестного заражения минимизирована.
- Заранее планировать визиты для технического обслуживания. Госорганы или компании могут ослаблять правила или делать исключения для обслуживания критического оборудования. Операторы должны заранее спланировать пути реализации ТО и получить необходимые разрешения, если таковые требуются.

Управление сменами

В идеале принципы резервирования, используемые для архитектуры и процедур эксплуатации ЦОДов, должны равным образом применяться и к персоналу. На многих площадках, разумеется, такие принципы уже реализованы. Во время эпидемии рекомендуется следующее:

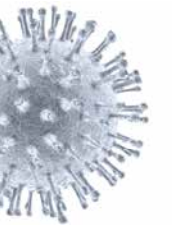
- Создать команды ответственного персонала, убедившись, что у каждой команды есть необходимые навыки и опыт, достаточный для эффективного управления объектом. Разделить команды между площадками, не допуская перемещений между площадками и исключая контакты персонала, работающего на основной площадке, с персоналом резервной площадки. По возможности организовать задачи таким образом, чтобы команды работали в отдельных зонах объекта, не входя в контакт друг с другом и не посещая рабочих пространств другой команды.
- Убедиться, что члены одной команды всегда работают в одной и той же смене, исключив таким образом любые контакты с другими сменами. Не допускать близкого взаимодействия между сменами. Приходящие на смену работники должны сохранять дистанцию по крайней мере 2 м с уходящими работниками. Это относится, в частности, к их передвижению в лифтах. Разделяемые рабочие пространства заступающий на смену персонал должен протирать дезинфицирующими салфетками. Согласно рекомендациям медицинского персонала или руководства, работникам следует использовать маски во время смены.
- Внедрить систему отслеживания контактов. Ежедневно регистрировать информацию о состоянии здоровья и местонахождении персонала, представителей поставщиков и прочих вовлеченных лиц, чтобы не пропустить проявление заражения коронавирусом или любые другие болезненные симптомы (в том числе обычной простуды).



Защита эксплуатации объекта

Чтобы гарантировать поддержание высокого уровня доступности ЦОДа, в части эксплуатационных процессов рекомендуем следующее:

- В соответствии с лучшими практиками отрасли разбить задачи на критические и некритические для облегчения расстановки приоритетов.
- Отложить все несущественное обслуживание (например, ежеквартальное обслуживание системы управления электроснабжением) и значительные проекты, насколько это возможно.
- Если это несущественно, отложить высокорисковое тестирование (например, проведение «холодных» пусков и имитацию отключения внешнего питания) до того времени, когда риски пандемии сойдут на нет.
- Пересмотреть планы аварийного восстановления, стандартные и аварийные эксплуатационные процедуры, методики их исполнения, приоритеты и т.д. и обновлять их по мере необходимости с учетом текущих условий и прогноза их изменения.
- Проводить тренинги для поставщиков (удаленно, по мере возможности), чтобы они могли выполнить основные эксплуатационные процедуры в случае 100%-ного невыхода на работу основного персонала ЦОДа.
- Подготовиться к нарушениям цепочки поставок компонентов, таких как элементы кабельной разводки, серверные стойки, критические запчасти и др. Создать ЗИП большего объема, чем обычно.
- Разработать план действий для ситуаций, когда при отказе ключевого оборудования у вас может не оказаться необходимых ресурсов вследствие нарушения цепочки поставок.
- Убедиться, что установленные процедуры на случай выхода из строя оборудования ясны и доведены до персонала. Пересмотреть аварийные эксплуатационные процедуры и убедиться, что они ясно описывают как то, что должно быть сделано, чтобы гарантированно привести отказавшее оборудование в безопасное состояние (когда ремонт невозможен),



так и то, что должно быть исполнено для обеспечения непрерывности работ (например, переключение на обходные цепи, переход на резервные компоненты, миграция нагрузок и/или критических приложений на резервные ресурсы).

- Исследовать устойчивость архитектуры ЦОДа – если уровень резервирования недостаточен для продолжения работы при выходе из строя одного или нескольких компонентов, рассмотреть альтернативный план действий, гарантирующий сохранение доступности.
- Максимально заполнить топливные емкости.
- Иметь в резерве альтернативный вариант комплектования штата персонала (если это возможно и экономически оправданно).

Факторы, повышающие риск

Повседневные задачи, которые выполняются опытным собственным персоналом, хорошо знакомым с рабочей средой, имеют самые низкие риски. Операторам ЦОДов рекомендуется попытаться устранить внешние факторы, процессы и действия, которые привносят неопределенность. Обратите внимание на следующие моменты.

Присутствие на объекте консультантов и представителей поставщиков

- Устраните (насколько возможно) доступ всех поставщиков, присутствие которых не является необходимым, и отслеживайте тех, кто должен присутствовать.
- Пересмотрите программу обучения поставщиков и включите в нее информирование о расширенных процедурах охраны здоровья, обеспечения безопасности и правилах работы площадки.
- Если присутствие на объекте консультанта или иного внешнего лица необходимо, выделите уборные исключительно для посетителей и проводите полную уборку по окончанию визита. Запретите посетителям приносить еду на объект и использовать комнаты отдыха сотрудников.

Стороннее управление объектом и другие сторонние сервисы

Согласно исследованию Uptime Institute, две трети всех площадок используют сторонние сервисы (аутсорсинг). Необходима четкая координация между всеми заинтересованными компаниями, чтобы персонал не был дезориентирован противоречивыми указаниями. Предусмотрите следующее:

- Вместе с партнерами проработайте политики реагирования и процедуры эскалации.
- Определите периодичность и способы информирования всех сторон.
- Ознакомьтесь с условиями всех соглашений SLA в отношении численности персонала в смену и других показателей. Обсудите с партнерами их способность выполнить SLA.
- Обсудите заранее, смогут ли поставщики услуг восполнить недостаток локального персонала путем перевода опытных работников из другого региона.

ЦОДы в районах сильного поражения

Многие действия, описанные в этом документе, определяются самой компанией, но объекты, работающие в зонах сильного поражения, могут быть подчинены внешним государственным ограничениям. В таких зонах разумно применять самые строгие правила.

Ужесточите правила доступа посетителей:

- Введите предварительный осмотр всех запланированных посетителей до их появления на объекте.
- Отправляйте посетителям опросные листы по электронной почте за 48 ч до посещения (или еще раньше) и требуйте их заполнения до подтверждения визита. Убедитесь, что все ответы остаются актуальными на момент прибытия. Разрешайте посещение, только если ответы указывают на низкую вероятность инфицирования.
- Запретите незапланированные посещения.
- Введите проверку температуры (с использованием бесконтактных термометров) до входа на объект.

Установите дополнительные правила организации работы сотрудников:

- По возможности назначьте по крайней мере одного самоизолированного сотрудника по каждой позиции в каждой смене для вызова при ЧС.
- Учитывая, что инкубационный период заболевания COVID-19, как полагают, составляет две недели, предусмотрите двухнедельную ротацию рабочих смен: команда А работает в отдельной области без пересечения с другими командами в течение двух недель. Затем в течение следующих двух недель на место команды А заступает команда В, а команда А отправляется на двухнедельный карантин.
- Проанализируйте, как проходят обеденные перерывы персонала объекта. Выделите отдельного уборщика исключительно для поддержания гигиены комнаты отдыха. Закройте кафетерии и кухонные зоны.

- Подготовьтесь к продолжительному размещению персонала на объекте, но используйте эту меру только в самом крайнем случае, так как в таких условиях вирус может распространяться быстрее.

Строительные работы на объекте

Для организаций, вовлеченных в строительство ЦОДа, работы по его расширению в условиях пандемии представляют особую проблему. Скорость строительства сильно влияет на стоимость, и задержки в одной области работ могут повлиять как на многие другие области, так и на других поставщиков. Однако мы рекомендуем:

- Приостановить все несущественные проекты, если это возможно.
- Если проект должен продолжаться, координировать работу с подрядчиками таким образом, чтобы гарантировать, что все субподрядчики/поставщики применяют адекватные меры предосторожности.
- По возможности создать отдельный безопасный вход для всех участвующих в проекте сторон и изолировать персонал проекта от служб эксплуатации. Сотрудники, которым поручен надзор за исполнением проекта, должны заниматься только этим и не взаимодействовать с дежурным эксплуатационным персоналом.

Коммерческие ЦОДы

Коммерческие ЦОДы сталкиваются с большим числом посетителей, чем корпоративные. Это, в частности, действующие и потенциальные клиенты, а также различный обслуживающий персонал. Рекомендуем следующее:

- Отложите все осмотры, туры по ЦОДу и другие несущественные мероприятия на объекте.
- Во избежание неудобств и неудовлетворенности потенциальных клиентов действуйте проактивно: заранее проинформируйте их о плане готовности к COVID-19 и его влиянии на доступ на объект. В этих сообщениях следует подчеркнуть, что реализуемые шаги направлены на обеспечение максимальной доступности инфраструктуры ЦОДа ради блага клиентов.
- Информируйте клиентов о доступных технологиях, которые позволят им управлять рабочими нагрузками удаленно (например, удаленный мониторинг через средства DCIM, удаленные «умные» руки и т.п.).
- Ограничьте доступ к общим пространствам, таким как комнаты для клиентов и т.п. Убедитесь, что во всех общих зонах присутствуют средства санитарной обработки (и мусорные контейнеры), в том числе рядом с торговыми автоматами.

Объекты смешанного использования

Некоторые небольшие ЦОДы и серверные помещения располагаются в зданиях смешанного использования – офисных комплексах, производственных предприятиях или административных центрах. В этих случаях, хотя описанные в данном документе принципы применимы, правила обычно устанавливают руководители всего объекта. Поэтому очень важно четко прописать исключения из общих требований и правил пользования зданием в отношении обслуживания критической инфраструктуры и доступа к ней персонала.

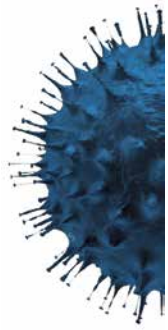
Общие рекомендации

Реагирование на уровне компании в целом

- Постоянно следите за ситуацией. Обращайтесь к доступным источникам информации за обновлениями и дополнительными указаниями.
- Делитесь опытом. В частности, ЦОДам в районах, менее затронутых пандемией, важно получать информацию от ЦОДов, оказавшихся в регионах с более тяжелой ситуацией, чтобы лучше подготовиться.
- Держите документацию наготове. Всегда может потребоваться получить разрешение ключевым сотрудникам ездить на работу (особенно если в районе ограничено перемещение).
- Разъясните процесс эскалации. Убедитесь, что бизнес-подразделения, особенно критически важные, полностью проинформированы об уровнях реагирования и конкретных событиях, которые могут потребовать эскалации.
- Удостоверьтесь в согласованных действиях бизнес- и технических подразделений. Требуйте, чтобы бизнес-подразделения чаще общались со службой эксплуатации ЦОДа и ИТ-отделом относительно изменений политик, влияющих на работу ЦОДа/ИТ-служб, например, о направлении сотрудников на удаленную работу или предписании клиентам использовать онлайн-сервисы.

Реагирование на уровне ЦОДа

- Пересмотрите приоритеты технического обслуживания. Определите, какие задачи могут быть понижены в приоритете, выполнены в последнюю очередь или не выполнены вообще, ес-



ли эксплуатационный персонал будет сокращен до минимума.

- Убедитесь в эффективности коммуникационных средств. Установите правила, согласно которым команды, изолированные друг от друга, будут вести общение (телефон, видеоконференция) на регулярной основе, и протестируйте средства коммуникации заранее.
- Избегайте совместного использования рабочего пространства. По возможности выделяйте разные помещения для персонала смен: например, дневная смена занимает рабочий офис, вечерняя – комнату для переговоров, а ночная – офис руководителя объекта.
- Избегайте совместного использования оборудования. Предоставьте каждому сотруднику индивидуальные средства. Если оборудование должно быть использовано совместно (например, телефоны смены, планшеты, клавиатуры и т.д.), дезинфицируйте его в начале каждой смены.

- Подготовьтесь к экстренному размещению персонала в ЦОДе. Хотя размещение персонала на объекте рекомендуется рассматривать только как крайнюю меру, перемещения могут быть заблокированы в середине смены, поэтому приготовьтесь к таким обстоятельствам.
- Заранее договоритесь с местными властями о том, чтобы ЦОД был определен как критический объект (подобно больнице или отделению полиции) и получите разрешения на перемещения для ответственного персонала. Разъясните критичность приложений, поддерживаемых площадкой (например, онлайн-банкинг, обеспечение связи и т.д.). Получите необходимые средства жизнеобеспечения – еду, основные гигиенические средства и медикаменты.
- Если возможно, найдите отель в непосредственной близости от площадки (в идеале – в шаговой доступности), который может быть использован для отдыха персонала между сменами.
- Пересмотрите вопросы отложенного обслуживания. Рассмотрите последствия отложенного обслуживания, поскольку оно может увеличить риск выхода из строя компонентов или систем. Всегда имейте в распоряжении план реагирования на любую значительную проблему, по мере необходимости координируя работу с поставщиками.
- Если проблему выхода оборудования из строя нельзя решить своевременно, убедитесь, что процедуры безопасного отключения и изолирования оборудования достаточно надежны для нейтрализации потерь (по крайней мере на время перевода рабочих нагрузок на другой объект).
- Поощряйте документирование и передачу знаний от опытного персонала; это может выполняться в форме аннотированных процедур и руководств, видеоконференций между соответствующими сторонами и т.д.
- Рассматривайте «восстановившийся» персонал как потенциально инфицированный и находящийся в зоне риска. Имеющаяся на сегодня информация указывает, что люди, преодолевшие заболевание и выздоровевшие, имеют лишь ограниченный иммунитет и могут заразиться повторно.

Выводы

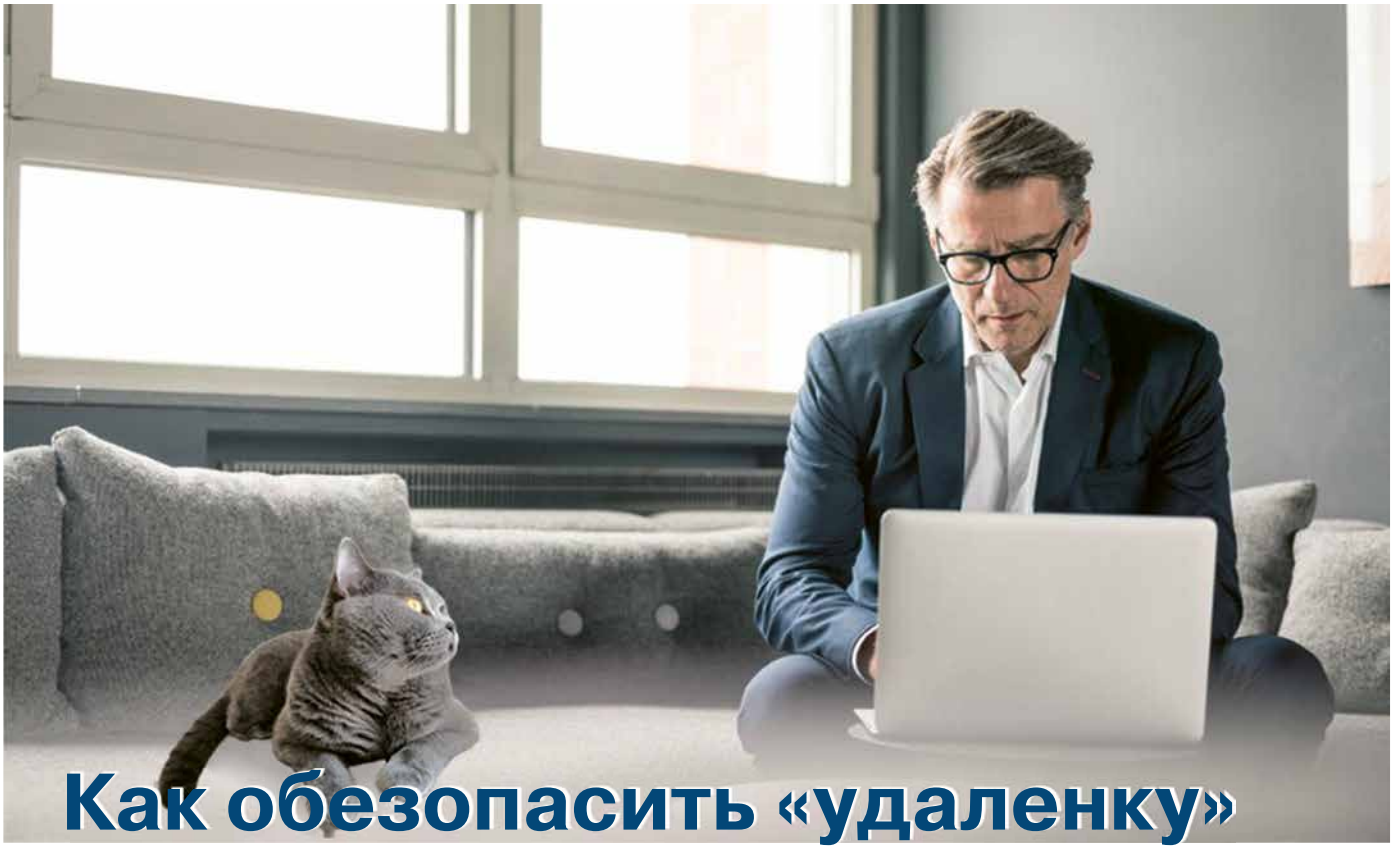
Многие из новых правил, введенных в действие в условиях пандемии, вероятно, будут навсегда включены в принципы управления критически важными объектами. Это может увеличить общие расходы.

Отрасль ЦОДов испытывает дефицит квалифицированного персонала. Текущие события заставляют индустрию, учебные заведения и коммерческие организации активнее заниматься подготовкой и обучением кадров.

Использование средств автоматизации и удаленного мониторинга может позволить объектам работать эффективнее, дольше и с меньшей численностью персонала. Пандемия усилит долгосрочную тенденцию более широкого внедрения таких средств. То же относится к инструментам удаленной совместной работы.

Эта пандемия не будет последней. За прошедшие двадцать лет различные вирусные вспышки уже вызывали массовые смерти и экономический спад. Глобализация означает, что таких эпидемий будет больше, и некоторые могут стать намного более смертоносными. Поэтому все организации должны быть подготовлены к ним, так же, как они готовы к более заурядным происшествиям, подобным перебоям в электроснабжении.

Есть предположение, что в дальнейшем вирус COVID-19, как грипп, будет давать ежегодные рецидивы. Планы обеспечения непрерывности бизнеса должны обновляться, включать новые профилактические меры (например, требование, чтобы ответственный персонал проходил прививки в начале каждого сезона гриппа) и меры по обеспечению устойчивости цифровых сред, резервированию площадок и т.д. ИКС



Как обезопасить «удаленку»

Пандемия COVID-19 повысила актуальность удаленной работы. Этот формат удобен и снижает вероятность заражения вирусом, но в то же время несет в себе ряд рисков, связанных с обеспечением информационной безопасности.

Денис Чигин, эксперт управления информационной безопасности, ГК Softline

Годами организации выстраивали информационную безопасность в рамках парадигмы, когда сотрудники работают в офисе – внутри контролируемого периметра. Часть сотрудников перемещалась между сетью организации и публичными и домашними сетями в силу специфики работы, но их доля была относительно невелика, и потому «удаленка» была более подконтрольна ИТ- и ИБ-департаментам. Сейчас же удаленные подключения стали массовыми, и организация безопасного доступа извне приобрела гораздо большую значимость. Кроме того, на новый тренд обратили внимание злоумышленники – по данным открытых источников, число целевых атак на организации в последнее время резко возросло.

Новые условия требуют изменения подхода к организации защиты информации. Распространить полный набор корпоративных средств защиты на домашние сети сотрудников невозможно, но существует ряд решений, позволяющих обезопасить работу из дома. Устройства, используемые для удаленного подключения, можно условно разделить на две группы: личные и корпоративные. Каждая из групп обладает своей спецификой. Личные устройства – это собственность пользователей, часто содержат личную или приватную информацию, что ограничивает нас в тех мерах, которые мы можем к ним применить. Обеспечение безопасности таких устройств требует особого подхода, но является решаемой задачей.

Защита личных устройств

Первым и наиболее важным шагом станет (если этого еще не было сделано) внедрение второго фактора аутентификации пользователей. Наиболее удобный вариант – мобильное приложение, которое будет генерировать для пользователя одноразовый пароль в дополнение к обычному паролю, что позволит существенно усложнить любые попытки взлома корпоративных ресурсов, которые в противном случае осуществлялись бы простым подбором пароля.

Второе средство защиты, которые мы бы рекомендовали к внедрению, – это капсулы. Абсолютное большинство пользователей и ранее имело доступ к почте и другим важным корпоративным ресурсам со своих мобильных

устройств, но сейчас вопрос защиты этих сервисов и информации, которую они могут содержать, стал более актуальным. Жесткие меры по защите информации для личных устройств могут оказаться избыточными, а само их применение может быть воспринято пользователями как вторжение в частную жизнь. Для решения этой задачи требуется средство, которое обеспечило бы безопасность информации на мобильных устройствах без подобных жестких мер. Капсульные решения дают возможность изолировать корпоративные приложения в специальной шифрованной области в памяти смартфона с тонкой настройкой того, что пользователь может с ними делать (запрет скриншотов, копирования, передачи файлов и пр.), что позволит обезопасить информацию, не влияя при этом на сложившиеся бизнес-процессы. При необходимости капсулы могут применяться и для корпоративных устройств.

Безопасность корпоративных устройств

Когда речь идет о корпоративных устройствах, наш инструментарий становится несколько шире. В отличие от личных, они всегда снабжены средствами защиты, например антивирусом. Остается лишь проконтролировать соответствие требованиям и политикам безопасности. Для этого можно использовать функционал проверки на соответствие (compliance), который содержат в себе многие агентские компоненты межсетевых экранов.

Как это работает? При попытке пользователя подключиться через VPN агент на его рабочей станции выполняет проверки: обновлена ли ОС до последней версии, используются ли наиболее свежие сигнатуры антивируса, не запущены ли приложения, которые находятся в черном списке и являются нежелательными в соответствии с политиками компании. Таким образом, хотя сам функционал и не является средством, которое непосредственно осуществляет защиту рабочей станции, он позволяет нам удостовериться, что все правила безопасности соблюдаются, и рабочая станция может получить доступ к корпоративным ресурсам.

Для того чтобы контролировать состояние корпоративных ноутбуков и смартфонов, разрешения для пользователей и общий уровень

РЕКОМЕНДАЦИИ ЭКСПЕРТА

Чек-лист: как организовать безопасную удаленную работу

Анна Михайлова,
системный архитектор, группа компаний Angara

Для того чтобы наладить удаленную работу с наибольшей эффективностью и наименьшими рисками, рекомендуем:

1. Не всех сотрудников переводить на работу через VPN-подключение. Некоторые рабочие обязанности могут выполняться с подключением только почты или других подобных облачных сервисов.

2. Для обмена документами организовать внутреннее или облачное файловое хранилище, доступ к которому обезопасить средствами защиты канала связи, строгой аутентификации и авторизации, желательно DLP-решением.

3. Ограничить канал связи: нет смысла направлять весь трафик пользователей через VPN-туннель. Это создаст лишнюю нагрузку на шлюз и внешний канал связи. Туннелировать весь трафик нужно лишь в определенных случаях (в зависимости от аттестационных требований к ИС, технических особенностей работы того или иного ПО и т.д.) и для определенных пользователей. Для остальных пользователей целесообразно применить политики узкой маршрутизации и порекомендовать им при работе в удаленном режиме не просматривать без необходимости мультимедиа-контент, а после окончания работы явно отключаться от VPN.

4. Запретить на уровне межсетевых экранов обмен с корпоративной средой лишним трафиком, скажем, трафиком SMB и Netbios. Если это невозможно, строго ограничить такой трафик до конкретного шлюза, размещенного в отдельном сегменте сети, обмен трафиком из которого с другими сегментами контролируется. Тогда в случае заражения удаленного пользовательского ПК, например, SMB-червем, вредоносное ПО, даже попав через VPN-туннель в корпоративную сеть, не распространится дальше и заразит только один сервер. Причем встроенный межсетевой экран имеют практически все клиенты удаленного доступа.

5. Если сотрудники работают на корпоративных ноутбуках, то следует реализовать проверку на соответствие политикам безопасности (compliance) при подключении устройств к сети: проверять актуальность антиви-

безопасности устройств, существует гораздо больше возможностей. Здесь логичнее применять решения класса MDM/EMM. Это позволит ИТ- и ИБ-отделам осуществлять контроль за тем, какие действия пользователей разрешены для таких устройств и какие приложения могут быть на них использованы, блокировать и сбрасывать настройки до заводских в случае кражи или потери устройства, чтобы предотвратить доступ злоумышленников к чувствительной информации, проверять, не рутовано ли устройство и выполнять в отношении таких устройств соответствующие действия.

В силу ограниченности средств защиты устройств пользователей в домашних и публичных сетях антивирусная защита приобретает особую важность. На корпоративных устройствах уже наверняка установлены агенты антивирусов, но в новых условиях их защитных механизмов может оказаться недостаточно. Поэтому целесообразно установить на корпоративные машины средства защиты, которые дополнили бы функционал антивирусного ПО, например, защитой от шифровальщиков или эксплойтов. Их применение расширит привычный инструментарий возможностью защиты от неизвестных угроз, что, в свою очередь, обеспечит безопасность корпоративных ресурсов при попытках атак на устройства пользователей.

Общие рекомендации

В сложившихся условиях важна тщательная настройка правил межсетевого экранирования и доступа пользователей к корпоративным ресурсам. Стоит вспомнить о возможности создавать политики межсетевого экранирования для определенного периода времени, ограничив временные рамки, в которые разрешен доступ извне (крайне сложно поверить в желание пользователя работать удаленно, скажем, в три часа ночи). Также всеобщий переход к «удаленке» – отличный повод для того, чтобы начать разрабатывать и применять у себя политику ZeroTrust, которая позволит уменьшить количество возможных векторов атаки, а значит, положительно скажется на общем уровне защищенности сети.

Для того чтобы выстроить систему защиты для удаленных подключений наиболее эффективно, можно воспользоваться помощью надежного сервисного провайдера с большим опытом работы в области ИБ. Эксперты специализированных компаний смогут подобрать и внедрить подходящие решения в соответствии с лучшими практиками и оказать техническую поддержку для того, чтобы снизить нагрузку на ИТ- и ИБ-отделы, которая резко возрастает в момент массового перехода к удаленной работе. ИКС

РЕКОМЕНДАЦИИ ЭКСПЕРТА

русной защиты и наличие необходимых пакетов обновлений, контролировать реестр процессов и автозапуска и др. При использовании личных ПК гарантировать выполнение пунктов политики безопасности на многообразии пользовательских устройств сложно. В таком случае следует проверить наличие минимальной защиты (антивирусное ПО, сканирование на известные вредоносные процессы) и снабдить пользователя инструкцией, как выполнять простейшие процедуры обеспечения безопасности: например, давать подтверждения, которые запрашивают некоторые VPN-клиенты, или использовать встроенные механизмы Microsoft (Microsoft Security Essentials).

6. Если есть возможность, лучше организовать работу конфиденциальных ИС через средства терминального доступа. Таким образом серверы защищаются от заражения и становится возможным даже применение политик контроля утечек (DLP).

7. Реализовать достаточный мониторинг работоспособности систем и событий ИБ для систем, использующихся при удаленном доступе, сбор событий доменной инфраструктуры и передачу их системам SOC и SIEM, а если возможно, то и SOAR.

8. С помощью систем класса User Behavioral Analytic организовать превентивную защиту от недобросовестных пользователей, попыток кражи информации и других неправомерных действий. Современные аналитические системы могут детектировать мошеннические действия, связанные с кражей данных, в режиме реального времени, используя алгоритмы Data Mining и/или Machine Learning. Правомерность доступа пользователя к данным может быть проверена алгоритмами, построенными на анализе аномальных запросов, и затем сопоставлена с общей

базой знаний для подтверждения результатов анализа и более точной классификации инцидента.

9. Для борьбы с утечками информации можно использовать DLP-системы в варианте удаленной работы и быстрого развертывания. Производители идут навстречу бизнесу ввиду мировой обстановки: например, компания Device Lock объявила о предоставлении своего ПО бесплатно в течение месяца (или более по запросу). Для развертывания системы наличие серверных ресурсов необязательно.

Контроль мобильных устройств: четыре подхода к решению

Алексей Парфентьев, руководитель отдела аналитики, «СёрчИнформ»

Компании по-прежнему плохо защищены от утечки данных через мобильные устройства. Однако представители бизнеса признают, что жертвуют мобильной безопасностью, чтобы выполнить работу быстрее. Что может быть разумным компромиссом в этой ситуации?

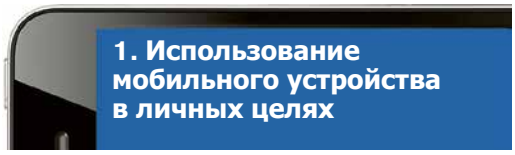
В 2019 г. число инцидентов с мобильными устройствами увеличилось на 5% по сравнению с 2018-м, говорится в ежегодном отчете Mobile Security Index 2019 крупнейшего американского оператора связи – компании Verizon.

В минувшем году от утечек данных через мобильные устройства пострадала каждая третья компания. Около 60% всех инцидентов были названы крупными, из них 40% – крупными с долгосрочными последствиями.

Люди не выпускают из рук гаджеты, а значит, число инцидентов будет только расти. Проблема усугубляется тем, что готового и универсального рецепта защиты дать почти невозможно.

Кроме зависимости людей от смартфонов из года в год растут и возможности последних. Они все быстрее передают данные, делают более качественные фотографии и видео, имеют более емкие запоминающие устройства, наполняются огромным количеством приложений. И, самое главное, они имеют доступ ко все более критичной информации о нашей жизни – данным кредитных карт, информации о состоянии здоровья, геоданным и т.д.

Чтобы правильно выбрать способы борьбы с угрозами, связанными с мобильными устройствами, необходимо определить типовые сценарии, реализацию которых мы хотим исключить или хотя бы минимизировать. Условно разделим их на три группы.



1. Использование мобильного устройства в личных целях

Зависимость от общения в мессенджерах и соцсетях, от игр и видео – бич нашего времени. Сотрудник может и не собираться «сливать» информацию или иначе вредить компании. Но если вместо работы он по три часа в день «сидит на ютубе», он также приносит убытки работодателю. Две трети компаний-респондентов из исследования Verizon заявили, что обеспокоены объемом непродуктивного мобильного трафика в их организации.

Но как определить, что именно делает пользователь в своем мобильном устройстве? Он ведь может, скажем, общаться с заказчиком или смотреть обучающее видео.

Для контроля трафика с мобильного устройства, подключенного к корпоративной ИТ-инфраструктуре, существует целый ряд решений:

- NGFW (межсетевые экраны нового поколения);
- связка из прокси-сервера и антивируса (для защиты от вредоносного ПО);
- связка из прокси-сервера и DLP-системы;
- DLP-система, интегрированная с корпоративными сервисами (например, с почтой).

Использование таких решений позволит не только ограничить доступ к нежелательному контенту или развлекательным сайтам, но и защититься от утечек чувствительной информации. Эти системы также могут ограничивать доступ к нежелательному, незаконному или вредоносному контенту.

Для того чтобы повысить дисциплину в организации, бывает достаточно самого факта развертывания решения для контроля мобильного трафика. У одного из наших заказчиков – компании с более чем 80 тыс. сотрудников – сразу же после внедрения средств контроля было зафиксировано, что использование мобильных каналов передачи данных в личных целях снизилось на треть. А доля времени, затрачиваемого на бизнес-приложения, значительно выросла. Просто сознавая, что мониторинг уже ведется, сотрудники изменили свое поведение на рабочем месте.

2. Небрежность и низкая грамотность при использовании устройств

Ежегодно в России крадут около 200 тыс. телефонов. Эксперты говорят, что в действительности эта цифра раз в пять больше, поскольку многие не заявляют о краже в полицию. Прибавьте сюда те устройства, которые люди просто теряют или по собственной воле вручают в разблокированном виде чужим людям, к примеру, мастерам по ремонту.

Неосторожность и небрежность сотрудника может стоить компании очень дорого, если ее данные хранятся на мобильных устройствах, особенно в незашифрованном виде.

Многие угрозы появляются также из-за неосторожности при работе с программным обеспечением, например, когда пользователь использует устаревшую операционную систему, открывает вредоносные ссылки или дает приложениям лишние разрешения. Единицы читают, что написано в пользовательском соглашении, большинство же не глядя нажимает «ОК» в ответ на просьбу приложения открыть доступ к геоданным или камере.

Отдельная тема – мобильный фишинг. Киберпреступники активно пользуются слабостями человека, воспринимающего мир через мобильное устройство, поэтому атаки через гаджеты стали не только массовыми, но и очень результативными.

По данным компании – разработчика антифишинговых решений Lookout, каждое четвертое приложение на мобильных телефонах их клиентов просит предоставить доступ к камере, который может быть использован для скрытого наблюдения, а микрофон – для прослушивания разговоров в компании. Даже доступ к календарю или списку контактов не безобиден. Похищенная контактная информация может задействоваться для фишинговой атаки с похожих адресов. Мошенники учитывают тот факт, что люди, скорее всего, откроют сообщение от знакомого человека.

Нет готовых решений, можно предложить только рекомендации. В первую очередь – внедрять программы для защиты от угроз на мобильных устройствах, блокировать нежелательные ресурсы на уровне сети. Во-вторых, проводить регулярные тренинги по информационной безопасности среди сотрудников. И наконец, ограничивать доступ личных девайсов в корпоративную инфраструктуру всегда, когда по работе это явно не требуется.

3. Намеренное киберпреступление с помощью мобильного устройства

Это самый опасный сценарий, ведь при таком развитии событий сотрудник будет исходить из личной выгоды и действовать осторожно.

Любой смартфон – это и переносное устройство хранения с огромным объемом памяти, и высокоскоростная точка Wi-Fi-доступа, и полноценный мобильный компьютер внутри корпоративной сети с соответствующими возможностями и уязвимостями. Есть прямой риск, что продвинутый пользователь будет использовать смартфон для обхода технических или административных регламентов. Например, подключать корпоративный ноутбук к собственному Wi-Fi, получая неконтролируемый выход в интернет.

Давайте признаем: современный мобильный гаджет – это идеальное орудие киберпреступления. Именно на предотвращение таких ситуаций и направлены основные усилия отделов информационной безопасности.

1) Ограничение на использование мобильных устройств на работе. Вы можете попросить сотрудников не пользоваться мобильниками на работе, но выполнят ли они просьбу? Что уж говорить о тех, кто действительно хочет украсть ценные сведения. Некоторые компании (особенно связанные с гостайной) практикуют сдачу сотрудниками мобильных телефонов на про-

ходных. Это, пожалуй, самый радикальный способ защиты, который при строгом контроле может быть эффективным. Но в эпоху интернета вещей, когда портативным устройством связи кроме телефона становятся самые разные предметы вроде наручных часов, очков или колец, этот способ защиты уже не работает. Любые бытовые предметы могут оказаться оружием мошенника.

2) Использование MDM/EMM-решений. Решения Mobile Device Management/Enterprise Mobility Management ограничивают возможность удаленного доступа к корпоративным информационным системам только для определенных устройств. Такой подход позволяет защитить информацию, но не спасает на 100% от ИТ-рисков типа распространения вредоносного ПО, передачи информации на телефон или с телефона через USB-интерфейс.

3) Комплексный контроль. Оптимальный подход – использовать компоненты DLP-систем. Например, для защиты от записи данных с компьютеров можно закрыть возможность подключения мобильных устройств к компьютерам и ноутбукам. Ноутбукам также можно запретить подключаться к Wi-Fi-сетям, которые сотрудник «раздает» с телефона или планшета. Кроме того, обеспечив высокоскоростной Wi-Fi-доступ для мобильных устройств в компании, можно контролировать мобильный трафик на сетевом уровне. Для этого нужно разрешить сотрудникам использовать корпоративный Wi-Fi на телефонах, и DLP-системы будут контролировать передаваемую по сети информацию.

4) Использование «глушилок». В России не запрещено использовать специальные подавители сотового сигнала, но их нужно зарегистрировать (вопросом занимается Государственная комиссия по радиочастотам). Устройства-«глушилки» создают плотные помехи на выбранной частоте (3G, LTE, 5G). Человек не сможет пользоваться сотовой сетью для передачи данных. Однако это должны делать специалисты и крайне аккуратно, поскольку есть риск полностью заблокировать связь, что вызовет недовольство и подозрения, а также навредит бизнес-процессам компании.

Но есть ситуации, когда «глушилки» незаменимы:

- в комнатах для деловых и секретных переговоров;
- на режимных и спецобъектах;
- в больницах – так как мобильные телефоны могут оказывать влияние на работу медицинского оборудования.

Угроза для корпоративной безопасности от неконтролируемого использования мобильных гаджетов становится все более актуальной. Решения на рынке есть, но ни одно из них не идеально. Выше перечислены только некоторые практики защиты, и каждой организации нужно делать выбор исходя из своего набора бизнес-процессов и данных. ИКС

3-я международная конференция и выставка

«ЦОД: модели, сервисы, инфраструктура»

26 ноября 2020, Екатеринбург, Hyatt Regency Ekaterinburg

Основные вопросы конференции:

- Аналитика iKS-Consulting. Анализ потребности УФО в дата-центрах
- Развитие рынка облачных услуг в РФ: Москва и регионы
- Мировые тренды в области развития сервисных моделей и инфраструктуры ЦОДов
- Современные технологии и решения для инженерной и ИТ-инфраструктуры ЦОДов
- Переход в облако. Опыт и новации
- Edge-ЦОДы для различных сегментов экономики
- Безопасность облачных решений и ЦОДов

Организатор

ИКС МЕДИА

Организатор

iKS CONSULTING

www.ekb.dcforum.ru

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

При поддержке

Минкомсвязь России

При участии

КООРДИНАЦИОННЫЙ СОВЕТ ПО ЦОДам И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ
Автономная некоммерческая организация

Uptime Institute®

Спонсоры и партнеры

RITTAL

ЗЕВС ЭЛЕКТРО

Janitza®

Группа Компаний ПОЖТЕХНИКА

Selectel

powerconcept BATTERY SOLUTIONS

www.iso-dist.ru
АЙСО-ДИСТРИБЬЮЦИЯ

Шкафы для настенного монтажа

Компания Schneider Electric анонсирует расширение линейки шкафов NetShelter WX. Новые модели предназначены для размещения активного и пассивного сетевого оборудования стандартной глубины при построении малых коммутационных узлов в проектах, где малые габариты, надежность и безопасность имеют первостепенное значение.

Шкафы NetShelter WX для настенного монтажа высотой 6U, 9U, 12U и 13U, глубиной 400 и 600 мм не требуют активной вентиляции – за счет перфорированной передней двери и перфорации на боковых стенках они обеспечивают пассивную конвекцию и бесшумное охлаждение установленного оборудования. Настенный монтаж позволяет компактно разместить телекоммуникационное оборудование, не занимая места на полу. Дверца шкафа открывается на 180 градусов, что упрощает и ускоряет процесс монтажа оборудования

Шкафы линейки NetShelter WX совместимы с широким ассортиментом продуктов Schneider Electric – ИБП, PDU, устройствами мониторинга семейства NetBotz и средствами организации кабелей, что обеспечивает необходимую функциональность для периферийных вычислений, включая удаленный контроль и управление доступом, видеонаблюдение и мониторинг окружающей среды. Поставляются в собранном виде.

Для быстрого конфигурирования комплексных решений на базе NetShelter WX можно воспользоваться утилитой Schneider Electric Local Edge Configurator.

www.schneider-electric.ru

Однофазные онлайн-ИБП

Компания ЦРИ «Импульс» обновила линейку однофазных онлайн-ИБП серии «Фристайл». Они представлены устройствами мощностью от 1 до 10 кВА.

Эта серия ИБП имеет универсальную конструкцию для стоечной и напольной установки. Глубина устройств значительно уменьшена по сравнению с предыдущим поколением «Фристайлов» и составляет всего 325 мм для моделей мощностью 1 кВА и 435 мм для моделей мощностью до 3 кВА, что устраняет необходимость выбирать более глубокие стойки только из-за ИБП, когда основное телекоммуникационное оборудование этого не требует.

Модели нового поколения 1–10 кВА имеют компактный корпус высотой 2U, оснащены полностью русифицированными поворотными ЖК-дисплеями, могут поставляться с различным коэффициентом выходной мощности (до 1,0). Входной диапазон напряжений находится в пределах 160--300 В. Встроенное зарядное устройство с возможностью коррекции фактора мощности может настраиваться через меню ИБП с максимальным зарядным током до 12 А (для заряда АКБ емкостью до 120 Ач).

Система управления ИБП построена с применением цифровых сигнальных процессоров (DSP) и обеспечивает функции самодиагностики.

Линейка ИБП «Фристайл» имеет энергоэффективность до 92% и весь перечень необходимых коммуникационных портов: последовательный порт RS232, HID USB, EPO, слот для установки дополнительных карт SNMP (для мониторинга устройства по Ethernet) и релейных карт (для коммуникации с широким спектром внешних устройств).

ИБП серии «Фристайл» могут быть укомплектованы встроенными батареями или иметь встроенное мощное зарядное устройство, позволяющее подключать к ИБП батареи большой емкости и обеспечивать длительное время автономной работы. Замена подключенных АКБ возможна в «горячем» режиме, без отключения питания нагрузки. Серия ИБП мощностью 1–3 кВА включает ряд моделей «Фристайл ЛФП» со встроенными или внешними литий-ионными ($LiFePO_4$) батареями.

www.impuls.energy

Система изоляции горячего/холодного воздуха

Компания Tripp Lite выпустила новый продукт линейки SmartRack – систему изоляции холодного/горячего воздуха для рядов стоек.

SmartRack Aisle Containment System – это модульное, простое в сборке решение для повышения эффективности охлаждения в центрах обработки данных, вычислительных узлах и серверных комнатах. Выбор типа внутренней зоны – холодная или горячая – определяется на этапе проектирования с учетом специфики помещения и существующей или планируемой к реализации системы кондиционирования.

Система изоляции состоит из нескольких элементов: торцевые опорные рамы (SRCTMTFRM), горизонтальные опорные балки (SRCTMTTLBM), панели крыши с прозрачными акриловыми вставками (SRCTMTCVR600), вертикальные панели и запираемые двойные двери с прозрачными акриловыми вставками (SRCTMTSDD). Решение включает в себя все необходимые материалы для сборки.

В минимальной конфигурации система изоляции может вмещать 8–12 шкафов (4–6 шкафов в каждом ряду) стандартной ширины 600 мм или 8–10 шкафов (4–5 шкафов в каждом ряду) шириной 750 мм и высотой 42, 45 или 48U. Для установки стоек разной высоты предусмотрены специальные адаптеры высоты. Если количество стоек в системе больше допустимого, то система наращивается таким же модулем. Решение совместимо с серверными стойками большинства производителей.

Требуемое количество компонентов базовой системы изоляции можно автоматически рассчитать на сайте производителя.

www.tripplite.ru

Универсальный мини-ЦОД

Компания ДКС выпустила новый продукт для ИТ-служб небольших предприятий – мини-ЦОД «NetOne 5-в-1». Это локальная инженерная инфраструктура, решающая задачу размещения активного и пассивного серверного и коммутационного оборудования, которое рассчитано на поддержку работы до 200 пользователей.

В моноблок NetOne интегрированы: система бесперебойного питания мощностью до 12 кВА, система распределения электропитания, кондиционер, система управления с доступом через веб-интерфейс, 42-юнитовый серверный шкаф и система противопожарной защиты. Все компоненты решения объединены в корпус со степенью пыле- и влагозащиты IP54 и размерами 2000 × 1100 × 1000 мм, что позволяет использовать продукт в том числе в производственных и запыленных помещениях. Передняя дверь из закаленного стекла облегчает визуальный контроль за установленным оборудованием. С тыльной стороны расположена двустворчатая сервисная дверь. Корпус размещается на цоколе высотой 100 мм. Кабельные вводы предусмотрены через крышу и цоколь.

Система управления инфраструктурой контролирует параметры работы кондиционера, ИБП, системы пожаротушения, а также влажность и температуру воздуха внутри шкафа и отправляет оповещения о выходе значений контролируемых параметров за допустимый диапазон.

Система автоматического газового пожаротушения R-Line использует огнетушащее вещество Novec 1230, обладающее нулевым потенциалом разрушения озонового слоя. Novec 1230 тушит огонь быстрее, чем инертные газы или тонкораспыленная вода, безопасно для электронного оборудования и не оставляет налета после пожаротушения.

Требуемая для установки мини-ЦОДа «NetOne 5-в-1» площадь составляет около 1,1 кв. м плюс небольшое пространство для открывания двери.

www.dkc.ru

РЕКЛАМА В НОМЕРЕ

СМАРТ КОНСТРАКШН
Тел.: (495) 280-7800
E-mail: info@smartc-sbrf.ru
http://smartc-sbrf.ru/.....с. 18–19

T8
Тел.: (495) 380-0179
E-mail: info@t8.ru
www.t8.ru.....с. 37

C3 SOLUTIONS
Тел.: (495) 133-1717
E-mail: info@c3solutions.ru
www.c3solutions.ru . . . . . 1-я обл., с. 60–61

HOSSER TELECOM SOLUTIONS
Тел.: (812) 363-11-93. Факс: (812) 363-11-94
E-mail: spb@h-ts.ru
www.h-ts.ru . . . . . с. 64–65

MITSUBISHI ELECTRIC
Тел.: (812) 449-5134
www.mitsubishi-aircon.ru . . . . . с. 49–51

RITTAL
Тел.: (495) 775-0230. Факс: (495) 775-0239
E-mail: info@rittal.ru
www.rittal.ru . . . . . с. 57, 58–59

SCHNEIDER ELECTRIC
Тел.: (495) 777-9990
Факс: (495) 777-9992
www.schneider-electric.com .. 2-я обл., ... с. 38–39

Указатель фирм и организаций

Учредители журнала «ИнформКурьер-Связь»:

ООО «ИКС-Медиа»:
105066, Москва
ул. Новорязанская, д. 31/7, корп. 14;
тел.: (495) 150-6424

МНТОРЭС им. А.С. Попова:
107031, Москва, ул. Рождественка,
д. 6/9/20, стр. 1;
тел.: (495) 921-1616.

IV ПРОФЕССИОНАЛЬНАЯ ПРЕМИЯ В ОБЛАСТИ ДАТА-ЦЕНТРОВ

RUSSIAN DATA CENTER AWARDS 2020

Торжественная церемония награждения состоится 22 сентября 2020 года

Премия Russian Data Center Awards позволяет выявить лучшие реализованные в России и странах СНГ проекты в области ЦОДов и облачных сервисов.

Жюри Премии состоит из известных российских и зарубежных экспертов, которые обладают многолетним опытом работы в отрасли дата-центров.

Получить информацию о номинациях и подать заявку на участие в конкурсе можно на сайте

DCAWARDS.RU

15-я международная конференция и выставка

ЦОД

22 сентября 2020
Москва, Центр Digital October

DATA CENTER FORUM

16+ Реклама

При поддержке

Минкомсвязь России

При участии

КООРДИНАЦИОННЫЙ СОВЕТ ПО ЦОДам И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ
Автономная некоммерческая организация

Uptime Institute

Спонсоры и партнеры

SberCloud · Life Is On Schneider Electric · HUAWEI · RITTAL · HTS · Группа Компаний ПОЖТЕХНИКА

mtu A Rolls-Royce solution · Atos · Allied Telesis · MITSUBISHI ELECTRIC Changes for the Better · ARISTA

DKC · HITEC Power Protection · C3 SOLUTIONS качественно.сделано.в России. · акционерное общество АБСОЛЮТНЫЕ ТЕХНОЛОГИИ · powerconcept BATTERY SOLUTIONS · ИМПУЛЬС источники бесперебойного питания