ИТ • Телеком • Медиа | www.iksmedia.ru | № 4 2020

ТЕМА НОМЕРА

ДОРОГИ PaaS

ИнформКурьер-Связь
ИКС
издается с 1992 года

Евгений Вирцер

Генеральный директор компании «Свободные Технологии Инжиниринг»

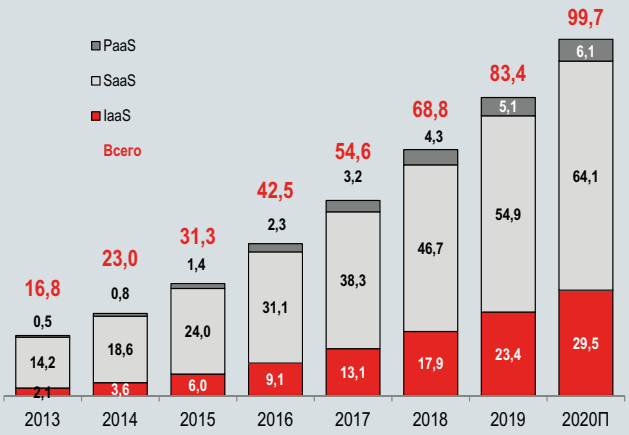
Рецепт успешного проекта ЦОДа

Аналитический отчет «Облачный провайдинг 2020»

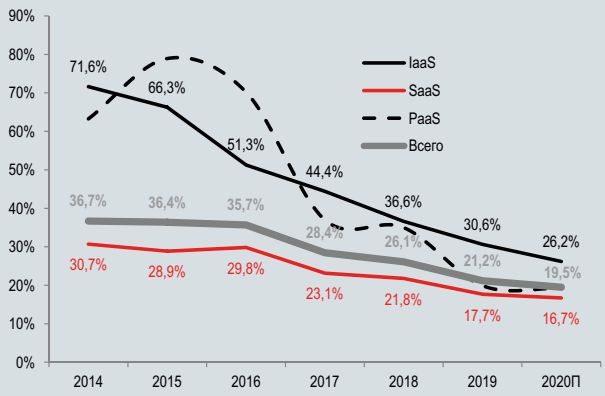
Отчет «Облачный провайдинг 2020» содержит результаты ежегодного исследования рынка облачных услуг в России. Он может быть интересен как игрокам рынка (провайдерам облачных услуг, дата-центрам), так и заказчикам услуг IaaS, PaaS и SaaS (телеком-операторам, банкам, страховым компаниям, ритейлерам и другим потенциальным пользователям облачных услуг). В отчете представлена информация об объеме и динамике российского рынка облачного провайдинга. На основе выделенных факторов развития рынка дан прогноз его роста до 2024 г. В ходе исследования проанализирована экосистема рынка. В отчете приводится карта, отражающая взаимодействие основных облачных провайдеров в России и дата-центров, предоставляющих услуги провайдерам. Рассмотрены основные сегменты IaaS, PaaS и SaaS.

В рамках исследования iKS-Consulting подготовил рейтинги провайдеров облачных услуг в целом и крупнейших игроков рынка в отдельных сегментах SaaS/IaaS/PaaS в 2019–2020 гг. Рейтинги включают оценку долей игроков в объеме доходов от услуг в каждом из сегментов рынка за 2019 г.

Рынок облачных услуг в России, 2013–2020 гг., млрд руб.



Темпы прироста сегментов облачного рынка в России в рублевом выражении, 2014–2020 гг., %



Параметры отчета
- Объем полной версии: около 200 с.
- Отчет содержит 22 таблицы, 137 графиков и диаграмм
- Исследование проведено в июле-октябре 2020 г.
- Язык отчета: русский
- Руководитель проекта: Станислав Мирин
- Стоимость полной версии: 198 000 руб. (без НДС)

Дополнительная информация и заказ отчета:
- E-mail: info@iks-consulting.ru
- Тел.: +7 (495) 150-6424

Структура отчета

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

№4/2020 подписан в печать 20.11.20.
Тираж 8 000 экз. Свободная цена.
Формат 64x84/8

ISSN 0869-7973

12+

Главная ценность ЦОДа

Пандемия обострила восприятие главных человеческих ценностей: свободы перемещения, семьи, здоровья, собственно жизни...

А что она показала в качестве главной ценности в индустрии ЦОДов? Недавно эксперты Uptime Institute опросили более 300 менеджеров дата-центров, чтобы выяснить, как новая реальность изменила их планы. И большинство ответило, что собираются повысить уровень отказоустойчивости своих ЦОДов, прекрасно понимая, что это потребует немалых средств.

Самоизоляция сотрудников, сокращение числа специалистов на площадке, сбои в работе цепочек поставок как оборудования, так и ресурсов, повышение нагрузки – это все принесла пандемия. В таких условиях ЦОДы должны продолжать бесперебойно функционировать, обеспечивая ИТ-сервисы, жизненно важные для экономики, медицины, государственного управления и социальной жизни. Большая часть ЦОДов справилась со своей задачей. Но даже самые искушенные футурологи не могут предсказать, что нас ждет далее, а значит, ЦОДы должны стать еще более устойчивыми – в том числе к неизвестным будущим вызовам.

При выборе коммерческих ЦОДов заказчики в России уделяют внимание в первую очередь базовым факторам, связанным с надежностью и отказоустойчивостью. Это показал опрос, проведенный в текущем году моими коллегами из iKS-Consulting. Кстати, согласно этому опросу, стоимость услуги по степени важности находится только на четвертом месте.

Если отталкиваться от системы уровней Tier, то по-настоящему отказоустойчивым является только ЦОД Tier IV. Несколько месяцев назад ИКС рассказывал о планах двух операторов – «РТК-ЦОД» и DataPro – построить такие ЦОДы в России. Ситуация развивается быстро. Аналогичные планы обнародовал еще один оператор – O2xygen.

Ближе всех к их реализации оказалась DataPro. В начале ноября компания заявила об открытии DataPro Moscow II – «первого дата-центра в Восточной Европе, соответствующего уровню надежности Tier IV». Совокупная мощность нового ЦОДа составит 1600 стойко-мест. Первая очередь на 800 стойко-мест уже введена в эксплуатацию, а вторая (еще на 800 стоек) станет доступна до конца 2020 г. Правда, пандемия внесла свои коррективы в график работ, не позволив пройти сертификацию на соответствие Tier IV к открытию ЦОДа. Однако компания планирует полностью завершить сертификацию в категориях Design и Facility в ближайшее время.

Развитие российской индустрии ЦОДов – это новые ИТ-сервисы, которые так необходимы всем нам, в том числе для функционирования экономики, сохранения здоровья и спасения жизней.

Берегите себя и своих близких,
Александр Барсков

ТЕМА НОМЕРА

Дороги PaaS

с. 66

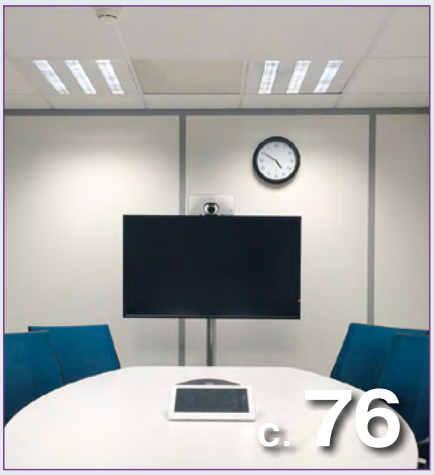
с. 7

Китайский тигр предлагает помощь России

с. 12

А. Барсков. Дорогие киловатты

А. Абрамов. Open RAN – имя нарицательное?



Б. Попов. Видеоконференцсвязь в России: правда, о которой не говорят

с. 86

М. Мустафаев. Взгляд на безопасность КИИ через облака

Регионы ждут ЦОДов

Региональные власти заинтересованы в появлении ЦОДов, но инвесторы подходят к выбору места для их строительства с осторожностью, опасаясь невысокого спроса на локальных рынках.

Так можно кратко сформулировать один из основных выводов организованной «ИКС-Медиа» онлайн-конференции «ЦОД. Регион», посвященной развитию цифровой инфраструктуры в регионах России. Использовался хорошо зарекомендовавший себя при проведении конференции Cloud & Digital Transformation 2020 формат – спикеры собрались в одной студии в Москве, а их выступления и дискуссии транслировались через интернет. Онлайн-формат положительно сказался на числе участников – конференция привлекла более 650 делегатов из разных регионов России и стран СНГ, причем большой интерес проявили региональные органы власти.

Кадр из видеотрансляции

Государство и ЦОДы

Объем генерируемых различными информационными системами данных стремительно растет, для их обработки нужны ЦОДы. Государство понимает важность строительства этих объектов в регионах, в том числе для реализации национальных проектов в рамках программы «Цифровая экономика РФ». Директор департамента инфраструктурных проектов Министерства цифрового развития, связи и массовых коммуникаций РФ Игорь Семенихин выделил здравоохранение, образование и обслуживание дорог как направления, требующие значительных вычислительных мощностей для обработки данных в регионах, и рассказал об обсуждаемых мерах поддержки их создания. Предлагается, например, направить часть бюджетов национальных проектов на коммерческий рынок центров обработки и хранения данных, что позволит до 2024 г. увеличивать объем рынка ЦОДов на 4–8 млрд руб. ежегодно.

В числе других мер – ужесточение требований по использованию российской инфраструктуры, разработка стандартов сертификации дата-центров и сокращение нормативных сроков технологических подключений к электросетям. По словам И. Семенихина, одна из проблем – сложность продвижения нововведений.

Впереди Москва

О необходимости строительства коммерческих ЦОДов в регионах, вблизи местных заказчиков, говорят с трибун конференций уже несколько лет, но пока процесс идет медленно. По данным iKS-Consulting, если в 2017 г. на Москву приходилось 68% стойко-мест, то в 2020-м – уже 72% (рис. 1). Ситуация понятная: в столице больше финансовых ресурсов и клиентов, а при выборе места для строительства коммерческого ЦОДа инвесторы смотрят прежде всего на потенциал спроса.

Тем не менее лед тронулся и в регионах. Прежде всего, силами «Ростелекома», который в ноябре 2019 г. в рамках федерального проекта ввел в эксплуатацию в Екатеринбурге первый созданный за пределами ЦФО опорный ЦОД своей сети. Причем на момент пуска вся емкость первой очереди дата-центра была уже зарезервирована

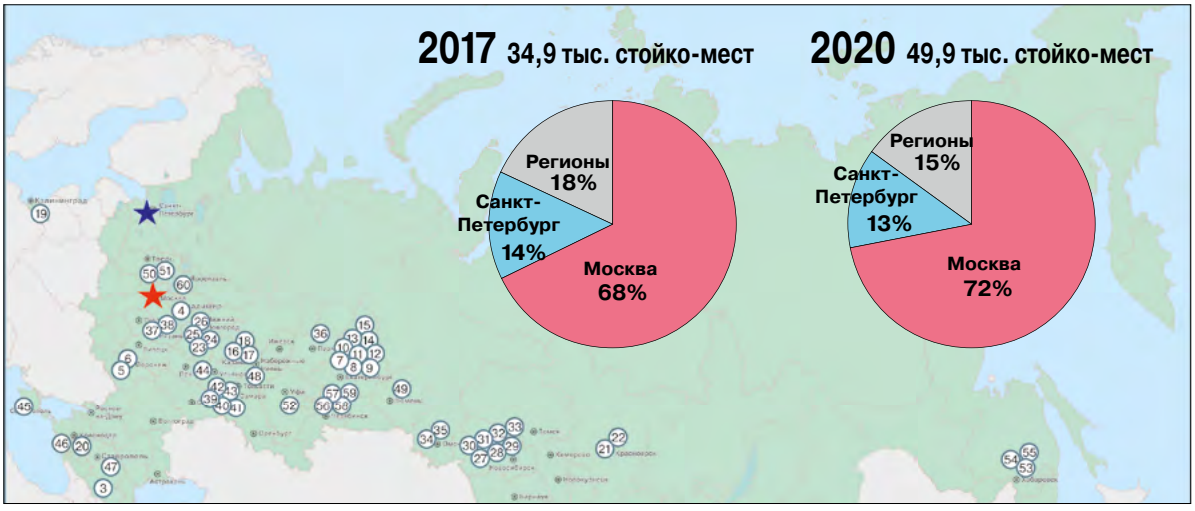
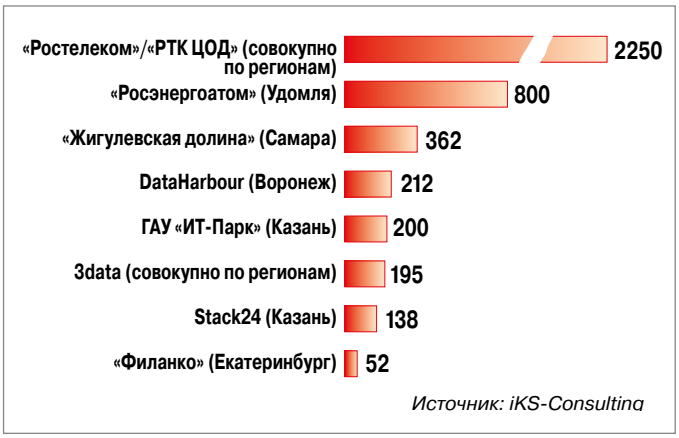


Рис. 1. Карта регионального рынка ЦОДов ▶

Источник: iKS-Consulting

заказчиками. К 2024 г. «опорные» – в терминологии «Ростелекома» – ЦОДы планируется создать во всех федеральных округах России.

«Ростелеком» занимает лидирующие позиции на рынке региональных коммерческих ЦОДов. Остальные компании отстают с большим отрывом (рис. 2).



▲ **Рис. 2. Крупнейшие коммерческие ЦОДы в регионах РФ**

Из столичных компаний ЦОДы в регионах начала строить 3data, которая использует модель франшизы. Агентство iKS-Consulting провело по заказу компании оценку целесообразности инвестиций в строительство ЦОДов в регионах, взяв в качестве критериев сетевую доступность, деловую активность, открытость и уровень конкуренции. Первые места в рейтинге заняли Московская, Свердловская и Новосибирская области. В Московской области 3data в декабре 2019 г. запустила ЦОД CA107 на пересечении Симферопольского шоссе и Московского малого кольца (A107, «малая бетонка»). В октябре нынешнего года планируется ввести в эксплуатацию ЦОД «Омск» емкостью до 200 серверных стоек. Как отметил генеральный директор 3data Илья Хала, это первый коммерческий ЦОД уровня Tier III в Омске, а возможно, и во всей Сибири.

В поисках инвесторов

При планировании создания коммерческого ЦОДа инвесторов в первую очередь интересуют гарантии наличия в регионе спроса на предоставляемые услуги. Лучше всего начинать строительство, имея «якорного» клиента, такого, каким стала «Газпром нефть» для ЦОДа «Ростелекома» в Екатеринбурге.

Первым быть трудно, надо с нуля формировать рынок, вести просветительскую работу, объяснять преимущества аутсорсинга ИТ и облачных вычислений. Важна поддержка администрации, причем не только содействие в получении разрешений и подключения к электросети, но и помощь в обеспечении спроса – например, в виде обязательств по переводу в ЦОД части региональных информационных систем.

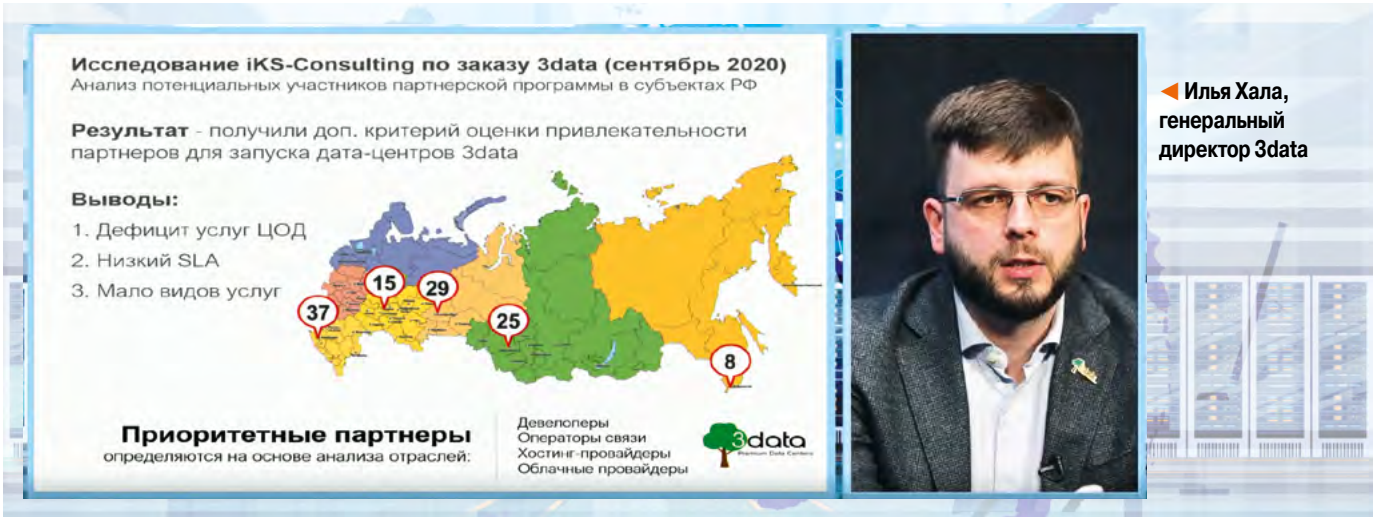
Серьезной проблемой является демпинг. Существующие региональные информационные системы сейчас где-то работают, пусть даже эти площадки трудно назвать ЦОДами. Некоторые региональные компании смотрят прежде всего на цену, не понимая, что серверная со свободным доступом посторонних, бытовым кондиционером на стене, отсутствием резервных каналов связи и линий электропитания – источник неизбежных отказов. А за размещение системы в высоконадежном ЦОДе надо платить совсем другие деньги. И понимать, что эти затраты за счет непрерывности бизнеса окупятся.

Если речь идет о корпоративных ЦОДах, то, как отметил директор проектов по строительству ЦОДов Сбербанка Сергей Шуршалин, наиболее важными критериями являются цена электричества (желательно меньше 2 руб. за 1 кВт), наличие местных квалифицированных кадров и налоговые льготы, например, в рамках особой экономической зоны.

И, конечно, для всех видов ЦОДов важны надежные скоростные каналы связи, чем больше – тем лучше.

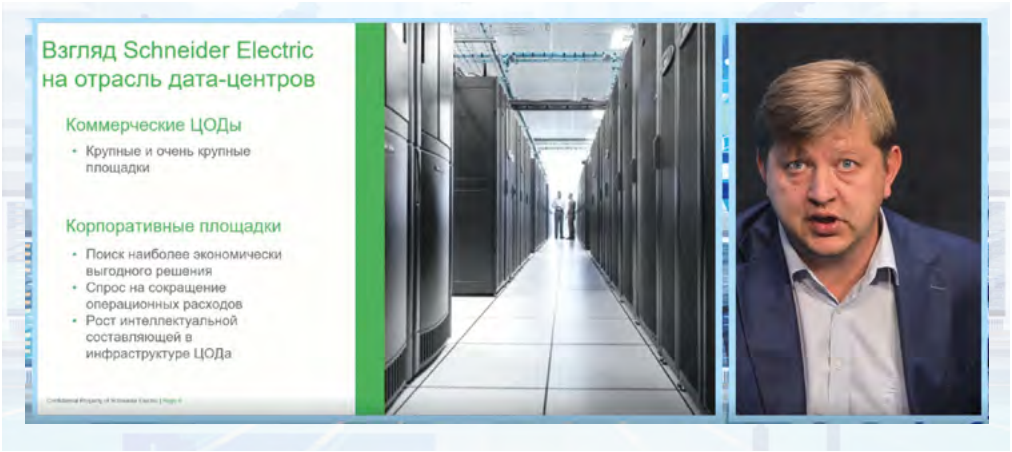
Оптимизация инженерной инфраструктуры

В техническом плане региональные ЦОДы не слишком отличаются от столичных. Разве что меньше число стоек, меньше клиентов, да и платежеспособность их зачастую ниже. Поэтому для обеспечения конкурентной цены придется приложить дополнительные усилия. Например, для ЦОДов с ограниченным бюджетом Schneider Electric предлагает специальные решения. Среди них новинка – источ-



Кадр из видеотрансляции

◀ **Илья Хала, генеральный директор 3data**



Кадр из видеотрансляции

◀ **Алексей Соловьев, технический директор подразделения Secure Power компании Schneider Electric**

ник бесперебойного питания Easy UPS 3M, который, по словам технического директора подразделения Secure Power компании Schneider Electric Алексея Соловьева, в режиме двойного преобразования имеет КПД до 95,5% и позиционируется как предложение, сбалансированное между первоначальными затратами и последующей экономией.

Перебои в энергоснабжении – одна из основных причин остановки ЦОДа. Но не стоит забывать и о других причинах. Например, о пожаре или ложном срабатывании систем пожаротушения.

Современные отечественные системы сверхраннего обнаружения дыма «Ионосенс ИПДА-1», о которых рассказал исполнительный директор ГК «Пожтехника» Антон Анненков, фиксируют выделяемые нагретыми проводами аэрозоли за сутки до пожара. Остается пройтись по проводам с тепловизором и найти проблемный участок. Как заявил А. Анненков, это первый прибор такого класса, произведенный в России.

Один из путей снижения стоимости регионального ЦОДа – использование стандартизированных решений. Например, небольших edge-ЦОДов, число которых, по мнению 53% опрошенных компанией Vertiv респондентов, к 2025 г. удвоится. Но уже сейчас, как сообщил КАМ Colo & Cloud Vertiv Евгений Журавлев, для российского банка, входящего в топ-5, компания развернула на своих типовых решениях с последующим подключением к общей системе мониторинга региональную сеть из более чем 500 офисов и филиалов.

Снизить операционные расходы дата-центра можно путем повышения температуры в серверных залах. По данным агентства US General Services Administration, увеличение рабочей температуры ИТ-оборудования на 1°C сокращает энергопотребление на 4%. Продакт-менеджер направления «Холодильные машины и вентиляция» компании Mitsubishi Electric Сергей Новиков порекомендовал использовать в российских ЦОДах новые холодильные машины NR-FC-Z, оптимизированные для высокой температуры в машзале. Такая установка в ЦОДе, расположенном в Лондоне, при рабочей температуре хладоносителя 28/20°C полностью удовлетворяет потребности ИТ-оборудования в охлаждении. При этом 50% времени задействуется только естественное охлаждение, а в течение 49% времени компрессоры работают при частичной нагрузке. Так что NR-FC-Z крайне редко функционирует в режиме обычной холодильной машины.

Что нельзя измерить – нельзя улучшить. Комплексные решения для энергоменеджмента и контроля качества электроэнергии представили на конференции компания Janitza Electronics и ее российский партнер «ЭЕВС-Электро». Приборы контролируют не только параметры электрической сети, но и характеристики воды, газа или пара, осуществляют контроль энергоэффективности ЦОДа на трех уровнях (в соответствии с европейским стандартом DIN EN 50600-2-2). Система позволяет оценить реальные потери энергии и выявить проблемные места в дата-центре.

Оптимизация использования ИТ-инфраструктуры

Снижения расходов можно добиться и за счет оптимизации вычислительной инфраструктуры. «Два основных вызова в ИТ – масштабируемость и изменяемость ресурсов», – отметил управляющий директор SUSE Владимир Главчев. Выход – абстрагироваться от «железа» и вынести выделение ресурсов на программный уровень с оркестрацией вычислительных мощностей, систем хранения и сети.

Платить за лицензии проприетарных программ или за сопровождение решений open source? В регионах зарплаты ниже, чем в столицах, поэтому сопровождение силами местных специалистов обойдется дешевле. Open source-решения давно доказали свою зрелость, широко используются бизнесом в мире, да и в реестр российского ПО включены в основном программы, созданные на базе open source.

Впрочем, в регионе квалифицированных специалистов может и не оказаться. В этом случае могут помочь программно-аппаратные комплексы Cisco UCS mini, оптимизированные для небольших региональных ЦОДов. Гиперконвергентная система быстро адаптируется к разным сценариям эксплуатации, а облачное решение Cisco Intersight позволяет управлять настройками удаленно через облако. Отвечая на вопросы об импортозамещении, старший архитектор по технологиям Cisco Евгений Логунцов пояснил, что существующее законодательство не мешает компании успешно работать на российском рынке, в том числе с органами государственной власти.

В целом конференция показала, что заинтересованность в строительстве ЦОДов в регионах у инвесторов и государства есть. Компаниям, вышедшим на региональные рынки ЦОДов первыми, придется нелегко, но при грамотном выборе места строительства и правильной бизнес-стратегии их усилия увенчаются успехом. ЦОДы в регионах будут – это неизбежно.

Николай Носов

Китайский тигр предлагает помощь России

В условиях санкций компания Huawei снижает зависимость от американских технологий и расширяет сотрудничество с Россией.

Борьба за лидерство

В 2017 г. Huawei заявила о главной стратегической задаче: попасть в список пяти компаний – разработчиков облачных платформ, на вычислительной инфраструктуре которых будет происходить цифровая трансформация мира. Общий подход – Huawei предоставляет платформу, инфраструктурные решения, технологии, а конкретные внедрения и сопровождение систем, работающих в рамках экосистемы китайского гиганта, осуществляют локальные партнеры в разных частях мира.

Процесс пошел. По словам исполнительного директора компании Го Пина, запись выступления которого открыла партнерскую конференцию Huawei «Цифровое сообщество 2020» в Москве, за прошедшие три года компания охватила 23 региона мира и подключила к своей облачной платформе более полутора миллионов разработчиков.

Особое место в планах Huawei занимает Россия. В 2018 г. в Москве компания открыла одну из своих лабораторий OpenLab, которые являются связующим звеном с независимыми разработчиками и локальными интеграторами. Весной 2018 г. Huawei запустила публичное российское облако Huawei 3data Cloud – первое публичное облако под брендом компании за пределами Китая. В дальнейшем Huawei перешла к обкатанной на локальных рынках других стран стратегии – предоставлению сервисов под брендом локального игрока – и начала сотрудничество с облачным провайдером SberCloud.

Эйден У

«Россия славится на весь мир разработчиками программного обеспечения и приложений, – отметил президент Huawei в регионе Евразия Эйден У. – Многие из них обладают уникальными преимуществами, например, “Яндекс” в сфере ИИ и приложений, “Лаборатория Касперского” в области кибербезопасности, “1С” в сфере финансового ПО. Россия находится в верхних строчках в глобальном рейтинге в области фундаментальных исследований, доказательством чему служит 21 российский лауреат Нобелевской премии. Между тем компания Huawei располагает передовыми аппаратными и программными платформами в области подключения, вычислений и устройств». Другая сильная сторона Huawei – способность находить практическое применение научным разработкам.

«Если мы объединим наши преимущества, то, несомненно, ускорим внедрение российских научных исследований в производство, от чего выиграет не только Россия, но и весь мир», – подчеркнул Эйден У, предложивший на партнерской конференции концепцию T.I.G.E.R. «T» (Technology) означает общие технологии. Компания планирует открыть ОС Harmony, ОС OpenEuler и систему управления реляционными базами данных OpenGauss для России. «I» (Industry) – общая индустрия. Компания готова предоставить передовые отраслевые решения нашей стране. «G» (Growth) – общий рост, коммерческий успех на рынке. «E» (Ecosystem) – общие экосистемы в области коммуникационных технологий, устройств и облаков. Примером может служить сотрудничество с экосистемой «Сбера» в части облачных вычислений. «R» (Reliability) – общая надежность.

В течение следующих пяти лет Huawei планирует подготовить свыше 130 тыс. российских специалистов в области цифровых технологий, выделить более $1 млрд на локальные закупки, исследования и разработки, а также создание экосистем для развития цифрового сообщества.

Го Пин

Владимир Рубанов рассказывает о Harmony OS 2.0

Импортозамещение по-китайски

Война санкций показала уязвимость бизнеса для запретов на использование зарубежных технологий. В черный список Министерства торговли США попала и компания Huawei, которой запретили приобретать без специальной лицензии полупроводники, включая микросхемы, произведенные иностранными фирмами, которые были разработаны или произведены с использованием американского программного обеспечения или технологий. Об отказе от сотрудничества с Huawei заявила и владеющая лицензией на операционную систему Android компания Google.

Ответом стала операционная система Harmony, версия 2.0 которой была анонсирована на конференции. «Harmony не замена Android, а нечто большее, – заявил главный технический директор по разработке программного обеспечения R&D-подразделения Huawei в России Владимир Рубанов. – Это распределенная операционная система».

Виртуальная шина в распределенной среде объединяет различные устройства в одно «связанное устройство». Операционная система, как всегда, связывает приложения с аппаратной частью, но в данном случае аппаратной частью становится «связанное устройство», т.е. распределенная ОС разбрасывает по устройствам фрагменты выполняемых приложений. Используется конвергентная сеть, опирающаяся одновременно на Bluetooth- и Wi-Fi-каналы. Экосистема устройств обладает функциями самообнаружения, причем для работы ОС необязательно использовать устройства Huawei.

Поверх виртуальной шины работают распределенная файловая система и распределенная база данных. По всей группе устройств поддерживается распределенный поиск. Для приложений с повышенным уровнем защиты, например, имеющим доступ к деньгам, система может на одном устройстве запросить пароль, на другом – распознать лицо, на третьем снять отпечатки пальцев. Для файлов и устройств используется мандатная система безопасности – колонка, имеющая низкий уровень доступа, не сможет взломать смартфон.

Пример использования распределенной системы: учитель выводит с телефона на планшеты и телевизор приложение, которое одновременно работает на всех устройствах в классе. Все гаджеты подключаются автоматически, ученики делают упражнения на планшетах, а учитель наблюдает за процессом по телевизору и помогает, отправляя сообщения.

Партнерство с Россией

Развивается партнерство Huawei с российскими компаниями. Облачная платформа Sbercloud.Advanced, развернутая на базе облачной платформы Huawei, предлагает уже более 40 платформенных сервисов. «Сбер» запустил сервис NFC-платежей, за 11 дней число скачиваний приложения «Сбербанк Онлайн» в магазине AppGallery достигло 3,2 млн, а к августу 2020 г. – 21 млн. Представители компании «Вымпелком» рассказали об успешной реализации пилотного проекта сети 5G на Абаканском горнодобывающем разрезе, позволившей добиться круглосуточного движения в автоматическом режиме «умных» БелАЗов, оснащенных модемами 5G и видеокамерами с высоким разрешением, по сложному, постоянно меняющемуся рельефу.

В силу геополитических причин мир раскалывается, причем и на технологическом уровне тоже. Китай и Россия оказываются по одну сторону разлома. Уже сейчас российское импортозамещение зачастую сводится к замене западного, несущего санкционные риски оборудования, на менее рискованное китайское.

Huawei нужны рынок сбыта и мозги российских разработчиков. Инвестиции в российское образование – не только инвестиции в будущих клиентов компании, но и повышение профессионального уровня студентов. Переманивание высокими зарплатами российских разработчиков – вызов для наших компаний, но в то же время создание в стране рабочих мест.

России нужен доступ к новым технологиям, прежде всего в микроэлектронике, где мы серьезно отстаем. Один из путей – локализация на территории России заводов по ее производству. Смогли же этого добиться в свое время китайцы от западных партнеров.

В мае 2020 г. Минпромторг подготовил проект постановления правительства, в котором говорилось о невозможности госзакупок иностранной радиоэлектроники при наличии аналогов отечественного производства. Созданная на локализованных заводах продукция – уже российская. Правительство РФ готово открыть компании Huawei доступ к госзакупкам, но при одном условии – китайский производитель предоставит нашей стране свои технологии, заявил директор департамента радиоэлектронной промышленности Минпромторга России Василий Шпак. По его словам, к концу сентября 2020 г. в процессе поиска путей сотрудничества правительство и руководство Huawei продвинулись не очень далеко, «но взаимный интерес есть», и диалог продолжается.

Го Пин закончил свое выступление на конференции цитатой Уолта Уитмена: «Всегда обращайте лицо к солнцу, и тени будут отставать от вас» – и призывом: «Давайте же в этом сложном полном неопределенности 2020 году обратим лица к солнцу и преодолеем трудности вместе». Предпосылки для сотрудничества Huawei с Россией есть, а как это сотрудничество будет развиваться на практике – покажет время.

Николай Носов

НОВОСТИ АНО КС ЦОД

АВГУСТ 2020

Рабочая встреча с вице-премьером правительства РФ

Представители АНО КС ЦОД приняли участие в рабочей встрече с вице-премьером правительства РФ Дмитрием Чернышенко, посвященной вопросам развития российской ИТ-индустрии, в том числе стимулированию развития отрасли ЦОДов. Позицию игроков рынка ЦОДов высказал Павел Каплунов, вице-президент «Ростелекома» и генеральный директор компании «РТК-ЦОД», члена АНО КС ЦОД.

СЕНТЯБРЬ 2020

АНО КС ЦОД на совещании, организованном ассоциацией «Цифровая энергетика»

В рамках мероприятия, собравшего более 60 участников, генеральный директор АНО КС ЦОД Дмитрий Бедердинов представил ряд предложений, касающихся оптимизации процессов технологического присоединения ЦОДов к электросетевым компаниям, а именно вариативного подхода при выборе поставщика электроэнергии, а также инициатив Минэкономразвития России по оплате резерва мощности. По результатам совещания предложения АНО были направлены для отражения в протоколе совещания, а также официальным письмом в Минцифры России.

ОКТЯБРЬ 2020

Подведены итоги исследования проблем технологического присоединения ЦОДов к энергосетевым компаниям

В опросе, проведенном АНО КС ЦОД, приняли участие представители операторов ЦОДов, эксплуатирующих 27 объектов общей мощностью около 180 МВт. Участники опроса указали, что время, фактически затраченное на подключение к электросетям, превысило запланированное. Для многих объектов такое превышение оказалось значительным, например, вместо шести месяцев – год или даже два. В среднем доля затрат на технологическое подключение ЦОДа к инфраструктуре ЭСК составляет примерно 12,3% общего объема капитальных затрат на создание ЦОДа. Для столичных объектов этот показатель превышает 15% (→ см. с. 12).

НОВОСТИ ОТРАСЛИ

«РТК-ЦОД» запустила модуль на 100 стоек, а рядом строит ЦОД Tier IV

Новый модуль расположен в здании дата-центра «Москва-I». Обслуживать его инфраструктуру будет объединенная команда «РТК-ЦОД» и DataLine. «Новый модуль уже принимает первых клиентов. По соседству с новым объектом полным ходом идет строительство дата-центра на 2000 стоек «Москва-IV», который мы будем сертифицировать по стандарту Uptime Institute Tier IV», – заявил генеральный директор «РТК-ЦОД» Павел Каплунов.

О планах относительно Tier IV заявила и O2xygen

Компания объявила о строительстве в Москве дата-центра нового поколения, в который собирается инвестировать около 2 млрд руб. Предполагается, что ЦОД получит сертификат надежности Tier IV и начнет работу в I квартале 2023 г. (первая очередь проекта). Площадь ЦОДа, который расположится в западной части российской столицы, составит 6 тыс. кв. м. Там планируется развернуть многофункциональную облачную инфраструктуру.

A DataPro уже построила ЦОД Tier IV

Фото: DataPro

По заявлению представителей компании, DataPro Moscow II – первый дата-центр в Восточной Европе, соответствующий уровню надежности Tier IV. В эксплуатацию введена первая очередь на 800 стойко-мест. Вторая очередь (еще на 800 стоек) станет доступна до конца 2020 г. Ограничения, связанные с карантином, не позволили пройти сертификацию на соответствие Tier IV к открытию дата-центра, однако ее (в категориях Design и Facility) планируется завершить в ближайшее время.

Совместный проект «Россетей» и «Росэнергоатома»

ГК «Россети» и концерн «Росэнергоатом» построят дата-центр на территории подстанции 500 кВ «Очаково» в Москве. В IV квартале 2020 г. должно быть подписано соглашение о реализации проекта, после чего начнутся проектно-изыскательские работы. Компании намерены создать специализированное совместное предприятие – оператора ЦОДа.

ЦОД 3data в Сибири

Столичная сеть дата-центров 3data запустила в Омске первый региональный ЦОД по модели франшизы. Центр обошелся местному партнеру в 400 млн руб. и будет обслуживать заказчиков Сибирского и Уральского федеральных округов.

Фото: 3data

Крупнейший ЦОД в Казахстане планируют сдать в эксплуатацию в 2023-м

Строительство ЦОДа продолжается в г. Петропавловске Северо-Казахстанской области. Новый объект появится на месте бывшего завода им. Калинина, территория которого не использовалась более 10 лет. Это один из проектов, вошедших в свободную экономическую зону Qyzyljar. Стоимость проекта – порядка 18 млрд тенге. Территория дата-центра – 26 га.

Большой ЦОД – под майнинг?

Глава Бурятии Алексей Цыденов подписал распоряжение о предоставлении компании «Битривер-Б» в аренду без проведения торгов земельного участка в с. Мухоршибири площадью 5,5 га. Земля выделяется для реализации масштабного инвестиционного проекта строительства дата-центра мощностью 100 МВт на территории опережающего развития «Бурятия».

ЦОДы – в стратегии развития Арктики

Формирование на севере Карелии сети центров обработки данных вошло в качестве одного из приоритетных направлений в утвержденную президентом России Стратегию развития Арктической зоны РФ и обеспечения национальной безопасности на период до 2035 г.

МТС построила первый на Северо-Западе модульный ЦОД

Строительство объекта в пос. Федоровское Ленинградской области велось в рамках соглашения между МТС и правительством Ленинградской области, заключенного в 2019 г. На первом этапе подведена мощность 8 МВт с возможностью увеличения до 16 МВт. Корпоративные клиенты и государственные заказчики региона смогут использовать инфраструктуру нового дата-центра в проектах системной интеграции, для хранения и обработки больших массивов данных, резервного копирования и переноса ИТ-систем на облачную платформу #CloudMTS.

Точка обмена трафиком – самый привлекательный партнер для ЦОДа

В нынешнем году исполнилось 25 лет со дня основания московской точки обмена трафиком MSK-IX. Об истории компании и о том, что она представляет собой сегодня, рассказывает Евгений Морозов, коммерческий директор «Центра взаимодействия компьютерных сетей МСК-IX».

– Прежде всего хочется поздравить компанию с юбилеем. 25 лет – огромный срок для российского рынка. Евгений, каковы причины создания компании и кто стоял у истоков?

– В 1995 г. семь провайдеров услуг доступа в интернет заключили соглашение об организации взаимного обмена IP-трафиком, чтобы абонент одного провайдера мог передавать данные абоненту другого. Для соединения каждого провайдера с каждым потребовалось бы проложить более двух десятков каналов и выделить инженерных работников для их администрирования. Подход далеко не оптимальный: эффективнее и надежнее создать единую точку обмена, упрощающую процессы администрирования, и для связи с другими провайдерами иметь всего один канал – до точки обмена трафиком.

Для того чтобы исключить возможность недобросовестных действий со стороны конкурентов, например, задержки передачи пакетов абонентов чужих сетей, провайдеры договорились о создании независимой нейтральной структуры. С этой целью обратились к специалистам РосНИИРОС – выходцам из Курчатовского института. Точка должна была отличаться высокой отказоустойчивостью, ведь все яйца складывались в одну корзину. Другое требование – масштабируемость, поскольку уже тогда было понятно, что экосистема будет разрастаться.

В то же время за рубежом появились другие крупные нейтральные точки обмена трафиком, лидирующие по сей день. Это AMS-IX в Амстердаме, LINX в Англии, DE-CIX во Франкфурте. Сегодня MSK-IX занимает четвертое место по объему трафика в Евразии и пятое в мире, уступая четвертое место точке обмена в Бразилии.

Первые коммутаторы «Московского Internet eXchange» (MSK-IX) установили на Московской междугородной телефонной станции № 9 (ММТС-9, М9), куда приходили международные и междугородные каналы связи и размещалось оборудование многих интернет-провайдеров. IX – это не только сокращение Internet eXchange, но и римская цифра «9». MSK-IX читалась как MSK-9 и у многих ассоциировалась с М9.

Новую компанию возглавил Алексей Павлович Платонов. В качестве коммерческого директора к проекту подключилась Елена Павловна Воронина, которая в настоящее время является генеральным директором «Центра взаимодействия компьютерных сетей МСК-IX».

– Как росла молодая компания?

– К площадкам в Курчатовском институте и на М9 добавились площадка ММТС-10 (М10) и другие точки подключения в Москве – «Центральный Телеграф», Вычислительный центр РЖД, Институт космических исследований, ГП «Космическая связь». Впоследствии стали подключаться появляющиеся на рынке коммерческие дата-центры – DataLine, DataPro, IXcellerate.

Следующий этап – региональное развитие. Точки обмена трафиком надо было создавать не только в Москве, но и в каждом федеральном округе. Появилась точка MSK-IX в Санкт-Петербурге, затем в Екатеринбурге, Новосибирске, Самаре, Ростове-на-Дону, Казани и Владивостоке. Региональные точки оптимизировали маршруты местного трафика: Екатеринбург – трафик Урала, Новосибирск – Сибири.

Ни одна точка не рождалась без контента. Ключевым партнером выступила компания «Яндекс», которой была интересна программа построения собственной региональной сети CDN для раздачи трафика. Раньше с периферии за контентом приходилось обращаться в Москву и платить за дорогие каналы связи. Теперь основную часть наиболее популярного контента «Яндекса» локальные пользователи получают из кэша, а цены в точках обмена трафиком в разы ниже, чем за IP-транзит.

Важным этапом развития компании стало появление услуги наземной доставки телесигнала, оказываемой на платформе медиалогистики. Телевизионный сигнал не терпит задержек и потерь. Резко выросли требования к качеству услуги, отражаемые в SLA, что привело к необходимости модернизации сети. В настоящее время MSK-IX передает картинку высокого качества, доставляет телевизионный сигнал не только по стране, но и за границу. В отношении медиалогистики MSK-IX опережает зарубежные точки обмена, даже европейские. Там соответствующая схема пока не выстроена, и поставщики контента не верят, что точка обмена может обеспечивать нужные характеристики.

– Как развивалось международное сотрудничество?

– MSK-IX с 2002 г. входит в ассоциацию Euro-IX. Участие в таком авторитетном экспертном сообществе повысило доверие со стороны зарубежных партнеров. В их число вошла, например, компания Akamai Technologies – крупнейший поставщик зарубежного контента.

MSK-IX «привела» в Россию компанию Google, первой стала с ней работать, помогла разместить оборудование на М9, предоставила шкафы и порты подключения. Это только

потом оборудование Google Global Cache начали устанавливать все интернет-провайдеры.

В последнее время активизировались китайские компании. Участниками MSK-IX стали Taobao, Alibaba и ряд крупных китайских корпораций, трафик которых постоянно растет.

Компания выступала принимающей стороной международной конференции ENOG/RIPE NCC Regional Meeting, регулярно участвует в международных технических и биллинговых форумах.

– Какие задачи решает компания? Как устроена MSK-IX на технологическом уровне?

– Сейчас у MSK-IX более 800 клиентов – интернет-компаний из 100 городов и 20 стран мира. У каждого оператора свое оборудование, и при использовании разнородного аппаратного обеспечения возникают ошибки. Мы делаем так, чтобы проблемы одного оператора не стали головной болью остальных.

Другая задача – защитить точку обмена MSK-IX от внешних воздействий. Для обеспечения надежной работы компания соединила несколько коммутаторов, расположенных в территориально разнесенных дата-центрах с подключением к разным узлам энергосети. Когда в мае 2005 г. в Москве случился блэкаут и точка на М9 отключилась, обмен трафиком продолжался благодаря точкам на севере столицы.

Изначально использовалась кольцевая топология – каждая точка обмена связана с двумя другими. Потом колец стало несколько. Компания настроила протокол, который позволял отключать поврежденные элементы кольца (например, из-за пожара в коллекторе) и переключать трафик на рабочие. Причем делалось это незаметно для участников обмена.

При кольцевой топологии один из оптоволоконных каналов не задействован, находится в резерве. Кроме того, сложно прогнозировать нагрузку на отдельные сегменты. В итоге компания перешла на работу с топологией «двойная звезда». В центре – два мощных коммутатора, расположенных на севере и на юге Москвы. Все точки обмена подключены к обоим коммутаторам. Используется протокол, позволяющий объединять обе «звезды».

С точки зрения топологии сеть выглядит как одна «звезда» с облаком из двух коммутаторов в центре. Схема надежная и позволяет на ходу проводить ремонт или обновление программного обеспечения. Она дает возможность прогнозировать распределение нагрузки и легко масштабируется – каждое плечо можно независимо расширять при увеличении трафика. Сеть спланирована с двукратным запасом нагрузки по каналам связи. Если загрузка больше 50%, то принимается решение о расширении канала.

– Как устроены точки обмена в регионах? Как они связаны?

– В региональных точках обмена объемы передаваемых данных меньше, и там пока достаточно кольцевой топологии. Каждый региональный узел подключен к двум разным провайдерам для мониторинга. Большая часть технических специалистов находится в Москве, но в точках присутствия в других городах есть инженеры, которые следят за состоянием оборудования, оперативно проводят кроссировки.

Основные российские и зарубежные контент-провайдеры находятся в Москве. Нет смысла передавать весь их трафик напрямую из столицы. Если запрос в Москву идет из Новосибирска через Екатеринбург, можно попробовать найти нужный контент в Екатеринбурге. Так строятся цепочки по стране, например, Владивосток – Новосибирск – Екатеринбург – Москва. Подобные цепочки экономически оправданы и минимизируют время отклика.

Инфраструктура MSK-IX включает в себя 41 узел, расположенный в 10 городах. К платформе подключено 566 автономных систем. Их контролируют операторы связи, интернет-компании, провайдеры CDN, хостинга и облачных сервисов, государственные организации, научные и образовательные учреждения. В октябре 2020 г. пиковый трафик через сеть MSK-IX достиг отметки 4,5 Тбит/с.

– Какие еще услуги предлагает компания рынку?

– Помимо пиринга на платформе Internet eXchange и доставки телесигналов на платформе «Медиалогистика», MSK-IX активно развивает платформу для быстрого и надежного доступа к сетям и облачным сервисам InstaNet. На базе платформы InstaNet предоставляются гарантированные локальные и междугородные каналы связи с надежностью до 99,9% и минимальными задержками, выделенные каналы для доступа к 10 российским и зарубежным облачным провайдерам, а также каналы для гарантированной доставки клиенту очищенного трафика от провайдеров услуг защиты от DDoS-атак.

MSK-IX продолжает совершенствовать распределенную платформу DNS-хостинга для доменных зон верхнего уровня. Платформа DNS MSK-IX используется администратором национальных доменов .ru и .рф, администраторами доменов верхнего уровня, госструктурами и компаниями, ведущими бизнес в интернете. Отказоустойчивость сервиса, зафиксированная в SLA, составляет 100%. Не многие сервисы могут похвастаться такой надежностью. Узлы платформы развернуты в 22 городах, причем не только в нашей стране, но и в Европе, Азии, Южной и Северной Америках.

– Каковы дальнейшие планы MSK-IX?

– Будущее за партнерствами! Мы дружим с дата-центрами, многие из них наши партнеры. Дата-центр оценивается клиентами по доступности, надежности и связности – количеству операторов, к которым можно подключиться. Точка обмена, размещенная в дата-центре, значительно увеличивает связность и привлекательность ЦОДа для клиентов. Рынок ЦОДов растет, и мы всегда открыты к новым партнерствам.

В то же время появляется все больше новых облачных сервисов. Компании переносят все больше важных функций в облака, и мы готовы обеспечить бесперебойную связь с облаком вне зависимости от перегрузок и маршрутизации в интернете. Мы планируем продолжать увеличивать количество как российских, так и зарубежных облачных сервисов, доступных для подключения на платформе InstaNet.

Дальнейшее развитие MSK-IX – коллаборация с сервисами в интернете для создания новых продуктов. Все хотят, чтобы их облачные сервисы были максимально доступны. В этом плане MSK-IX – один из наиболее привлекательных партнеров.

Дорогие киловатты

Александр Барсков

Большие временны́е и финансовые затраты дата-центров на технологическое подключение к электросетям и масштабирование мощности сдерживают развитие отрасли. А отсутствие выигрыша в стоимости электроэнергии уменьшает конкурентоспособность российских ЦОДов на мировом рынке.

Все, кто когда-либо занимался подключением даже небольшого объекта, например личного гаража, к электросети, знают, насколько это непросто, небыстро и недешево. Что уж говорить о ЦОДах. А ведь для них получение электропитания необходимой мощности – ключевое условие функционирования. Это не гараж, в который автомобиль можно поставить, освещая помещение светом фар, – что, кстати, мне приходилось делать почти год, пока длился процесс подключения. ЦОДы – важнейшие элементы цифровой инфраструктуры страны, стратегические объекты, способствующие реализации целого ряда национальных программ и повышению конкурентоспособности России. Тут сопоставление ЦОДа с гаражом даже неуместно, хотя, замечу, оба объекта можно использовать одинаково – для майнинга.

Техприсоединение: очень долго…

В сентябре 2020 г. АНО «Координационный совет по ЦОДам и облачным технологиям» (АНО КС ЦОД) провела исследование проблем, связанных с технологическим присоединением ЦОДов к сетям энергосетевых компаний (ЭСК). В опросе приняли участие представители российских операторов ЦОДов, эксплуатирующих 27 объектов общей мощностью около 180 МВт.

Почти все участники опроса указали, что время, фактически затраченное на подключение к электросетям, превзошло запланированное. Для многих объектов превышение оказалось значительным, например, вместо шести месяцев – год или даже два (рис. 1). Ни одному из операторов ЦОДов, участвовавших в опросе, не удалось реализовать такое подключение быстрее, чем за год.

Большая часть проблем при подключении к электрическим сетям впервые вводимых в эксплуатацию ЦОДов возникает, по сообщениям их операторов, при «осуществлении сетевой организацией фактического присоединения объектов заявителя». Некоторые операторы испытали затруднения уже на этапе подачи заявки на присоединение. Также операторы отметили высокую стоимость технологического присоединения, бюрократическую волокиту при обмене информацией, длительные сроки выполнения ТУ сетевой организацией («МОЭСК – два года, зачастую и в этот срок не укладываются») и проблемы при получении разрешения органа федерального государственного энергетического контроля на допуск к эксплуатации.

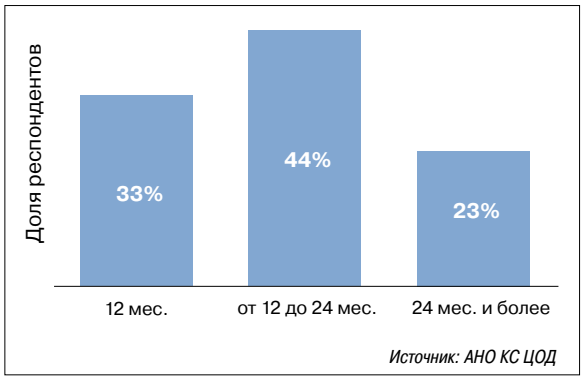
Хотя большинство операторов не сталкивались с прямым нарушением сетевыми компаниями законодательства, два респондента указали на «нарушение срока исполнения ТУ по договору техприсоединения» и «невыполнение сроков договора».

Резервирование/увеличение максимальной мощности ранее присоединенных ЦОДов также сопряжено с проблемами: длительными сроками осуществления присоединения, переносом сроков окончания работ, высокой стоимостью наращивания мощности.

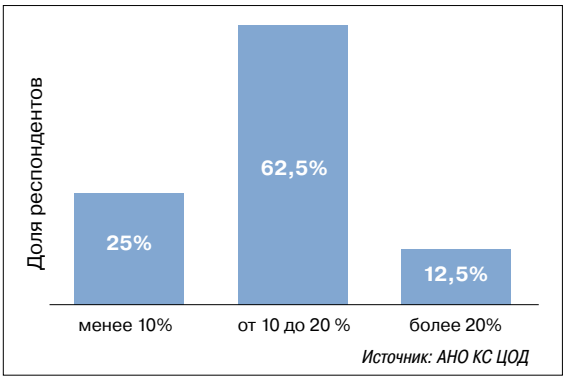
Согласитесь, даже год на присоединение – и это в лучшем случае – в наш стремительный век кажется неоправданно долгим сроком. А что говорит мировая практика? По словам сооснователя и CEO компании IXcellerate Гая Вилнера, признанного международного эксперта с 20-летним опытом построения ЦОДов в разных странах, в Германии и Франции национальные электросети имеют специальные отделы, работающие с ЦОДами для ускорения планирования и реализации подключений. В зависимости от возможностей систем генерации в конкретном месте и емкости электросети подключение (и наращивание мощности) ЦОДов может занять до шести месяцев, что в несколько раз меньше, чем в России.

…и очень дорого

Как уже упоминалось, практически все операторы ЦОДов жалуются не только на длительный срок, но и на высокую стоимость технологического присоединения (рис. 2). При этом, как отметили некоторые респонденты, «сетевая организация перекладывает расходы по реконструкции сетевой инфраструктуры на потребителя».



◀◀ Рис. 1.
Фактическое время, затраченное ЦОДами на подключение к ЭСК



◀ Рис. 2.
Доля затрат на подключение к ЭСК в общем объеме капзатрат на создание ЦОДа

В среднем затраты на технологическое подключение ЦОДа к инфраструктуре ЭСК составляют примерно 12,3% общего объема капитальных затрат на создание ЦОДа. Наименьшей эта доля оказалась у компаний, ЦОДы которых находятся не в Москве. Для столичных объектов данный показатель превышает 15%.

Энергетики рекомендуют ЦОДам выбирать точки присоединения так, чтобы оптимизировать его стоимость. Другими словами, строить ЦОДы рядом с генерирующими мощностями или там, где имеется избыток электроэнергии. Но мировой, да и российский опыт показывает, что ЦОДы являются не энергоцентричными, а клиентоцентричными объектами. И там, где нет спроса на энергию, скорее всего, не будет спроса и на услуги коммерческого ЦОДа.

Сравним приведенные выше цифры с данными по тем же Германии и Франции. В этих странах, по свидетельству Г. Вилнера, подключение к энергосистеме стоит в среднем 100 тыс. евро за 1 МВт. Если принять, что строительство типового ЦОДа в России обходится примерно в 40 тыс. евро за стойку мощностью 5 кВт, а средний коэффициент энергоэффективности (PUE) равен 1,5, то путем несложных вычислений получим, что у нас в стране стоимость такого подключения составляет около 650 тыс. евро, а в московском регионе превышает 800 тыс. евро, что в 8 (!) раз больше, чем в названных странах Европы. Понятно, что это оценочные расчеты, для конкретного объекта с учетом его особенностей и суммарной мощности превышение может оказаться не столь значительным. Но кратное превышение стоимости технологического подключения ЦОДов в России аналогичного показателя для Европы говорит о том, что ситуацию надо менять.

По нашим данным, для развернутого в Финляндии ЦОДа одной из крупных интернет-компаний технологическое подключение было осуществлено за три-четыре месяца и... бесплатно. Правда, компании пришлось оплатить строительство распределительной подстанции для этого подключения. Технологическое присоединение ЦОДа мощностью 24 МВт той же компании в центральной части России оказалось относительно недорогим (около 1,5 млн руб.), однако она была вынуждена за свои деньги (около 470 млн руб.) построить линию 110 кВ и понижающую подстанцию 110/20.

Как замечает генеральный директор DataPro Алексей Солдатов, с каждым годом затраты на технологическое подключение неуклонно растут, а сроки удлиняются.

В таких условиях сложно говорить о конкурентных преимуществах российской индустрии ЦОДов. Но, может быть, не все так грустно, ведь, как утверждают энергетики, «у нас существенно более низкая стоимость электроэнергии»? Давайте посмотрим.

Миф о дешевом электричестве

Как видно из исследования, проведенного KPMG, цена на электроэнергию в США и странах Европы в целом действительно выше, чем в России. Но для определенных групп потребителей она сопоставима, а зачастую и ниже (рис. 3). Здесь речь идет в первую очередь о квалифицированных энергоемких потребителях (КЭП), для которых регуляторы находят возможность снижать цену на электроэнергию, в частности, убирая из тарифа стоимость ее передачи.

КЭП – это специальная категория потребителей, конкурирующих на глобальных рынках, с особыми условиями ценообразования, включая

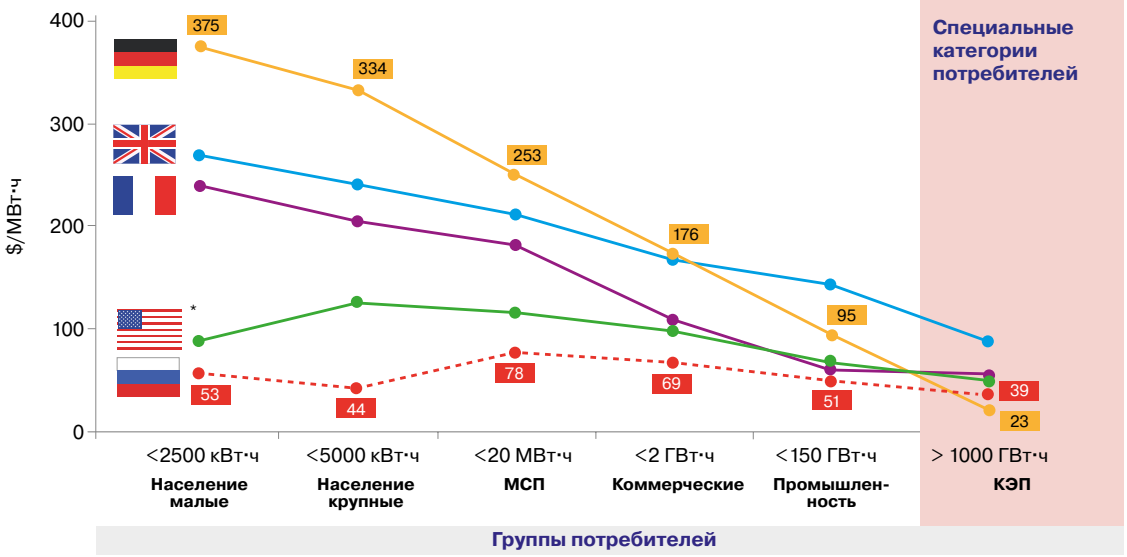


Рис. 3. ▶ Цены на электроэнергию в России и на зарубежных рынках

Источник: Евростат, EIA, анализ KPMG

* Данные приведены для компании PJM, отвечающей за функционирование оптового рынка электроэнергии, мощности и системных услуг на части или всей территории 13 штатов США и округа Колумбия.

освобождение от надбавок и сборов и сниженный тариф на транспортировку энергии вне зависимости от места технологического присоединения. Так, в Германии к КЭП относятся порядка 2 тыс. предприятий, на которые приходится примерно четверть всего потребления энергии в стране.

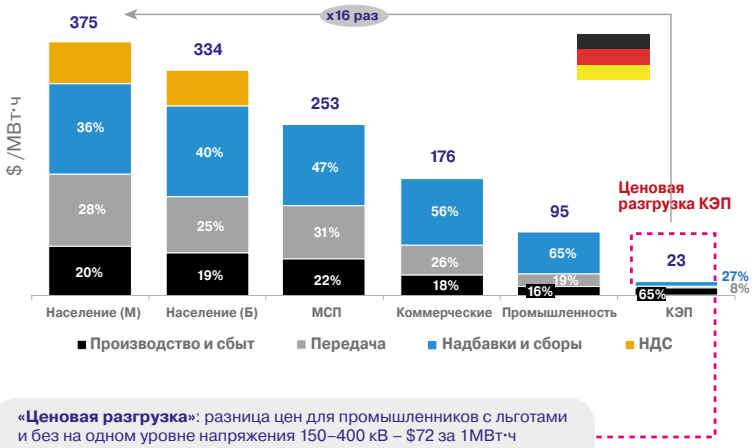
По данным, которые приводит Сергей Мигалин, заместитель генерального директора – директор по экономике и финансам концерна «Росэнергоатом», в странах Восточной Европы стоимость электричества (в Польше – 40 евро за 1 МВт·ч, в Болгарии – 30 евро за 1 МВт·ч) для таких потребителей, как ЦОДы, сопоставима со стоимостью электричества (32 евро за 1 МВт·ч) для ЦОДа «Калининский», находящегося рядом с Калининской АЭС и получающего его по оптовой цене. Понятно, что российским ЦОДам, энергетическое расположение которых не столь выгодно, как у «Калининского», электричество обходится дороже.

Из чего складывается стоимость электроэнергии, или На чем можно сэкономить

Если посмотреть на структуру цены на электроэнергию в Германии (рис. 4), то видно, что для КЭП ее снижение достигается главным образом за счет уменьшения сетевой составляющей, а также надбавок и сборов.

В России стоимость передачи составляет примерно 10% стоимости электроэнергии. Но эта величина зависит от того, подключается ли объект на правах оптового потребителя к Федеральной сетевой компании (ФСК ЕЭС), которая осуществляет передачу энергии по электросети РФ, или на правах розничного – к одной из межрегиональных распределительных сетевых компаний (МРСК), которые распределяют полученную от ФСК электроэнергию потребителям; обычно МРСК относятся к конкретному федеральному округу.

Разница оказывается существенной. В качестве примера С. Мигалин приводит цену электроэнергии для ЦОДа «Калининский», подключенного к ФСК, и прогноз цены на электроэнергию для ЦОДа, который мог бы быть развернут рядом с Кольской АЭС и подключен к МРСК. Хотя стоимость электроэнергии на Калининской АЭС в среднем на 25% выше, чем на Кольской АЭС, итоговая цена оказывается сопоставимой: 2851 руб. за 1 МВт·ч для ЦОДа рядом с Калининской АЭС и 2690 руб. за 1 МВт·ч для ЦОДа рядом с Кольской АЭС. По мнению заместителя генерального директора «Росэнергоатома», высокий тариф МРСК «съедает» все преимущества размещения ЦОДа в районе Кольской АЭС, несмотря даже на холодный климат, позволяющий существенно снизить расходы (как CAPEX, так



«Ценовая разгрузка»: разница цен для промышленников с льготами и без на одном уровне напряжения 150–400 кВ – $72 за 1МВт·ч за счет спец. регулирования надбавок и тарифов сетей

Источник: анализ KPMG

▲ Рис. 4. Структура конечных цен на электроэнергию в Германии (2019 г.)

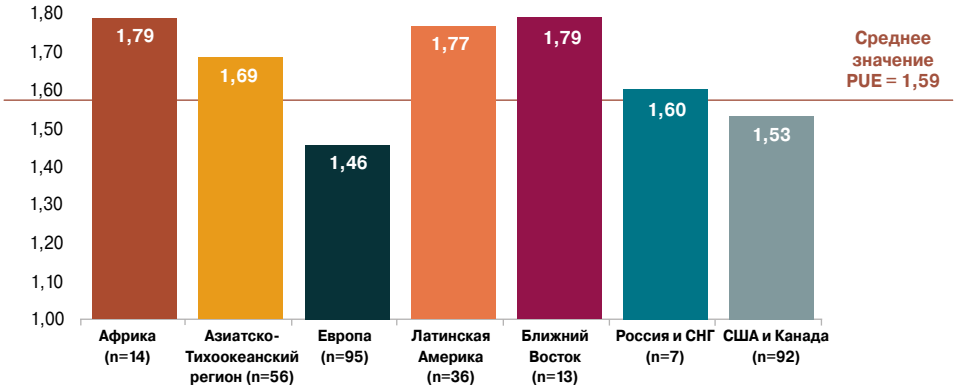
и OPEX) на систему охлаждения. «Получается, что рядом с Москвой [строить ЦОД] выгоднее, чем в арктической зоне», – заключает он.

Возможность для ЦОДов получать электроэнергию по оптовым ценам (подключаясь к ФСК по высокому напряжению) – один из путей снижения их расходов. Но на данный момент условием выхода компании на оптовый рынок электроэнергии и мощности является мощность от 20 МВт – порог для большинства ЦОДов высокий. Поэтому для реализации такой возможности требуется корректировка установленных правил, к чему энергетики пока не готовы.

Многие операторы ЦОДов считают, что оптимизировать стоимость электроэнергии для них может помочь исключение или гарантия уровня сетевой составляющей, которая сейчас постоянно увеличивается. Один из вариантов – подписание свободных договоров с заинтересованными сетевыми компаниями или генераторами (производителями энергии) с фиксированием сетевой надбавки на приемлемом уровне.

Сетевая надбавка взимается не только за доставку электроэнергии, но и за надежность энергообеспечения, которую гарантирует единая энергосистема России. Но для ЦОДов этой надежности недостаточно, они сами реализуют системы гарантированного и бесперебойного электропитания, используя дизель-генераторы и ИБП. Получается, что ЦОДы оплачивают ненужную им на деле гарантию, хотя это снижает их конкурентоспособность на мировом рынке. Примечательно, что в соответствии с российским законодательством об электроэнергетике ЦОДы не относятся к неотключаемым объектам, и аварийная бронь им не положена.

Когда речь заходит о возможности снижения тарифов, одним из аргументов энергетиков является повышение энергоэффективности: «Внедряйте новые энергоэффективные технологии, и доля непродуктивных затрат у вас уменьшится», – говорят они. Однако Видия Железнов, ди-



Источник: Uptime Institute, 2020

▲ Рис. 5. Среднее значение PUE крупнейших ЦОДов в различных регионах

ректор по стратегии и маркетинговым коммуникациям компании «РТК-ЦОД», констатирует: «Если посмотреть на данные энергоэффективности мировой отрасли ЦОДов, приводимые Uptime Institute (рис. 5), то видно, что среднеотраслевая энергоэффективность российских ЦОДов сопоставима с показателями США и Европы, и резервов снижения энергозатрат в этом направлении фактически нет».

Насколько важна цена?

Насколько существующая цена на электроэнергию является препятствием для развития рынка ЦОДов? По данным В. Железнова, при предоставлении услуг colocation доля стоимости электроэнергии в тарифе составляет примерно 25–35%. При этом, по результатам опросов iKS-Consulting среди потребителей услуг colocation, надежность электропитания (читай – непрерывность услуги) – на первом месте среди ключевых параметров для клиентов, а стоимость стойки – только на пятом (рис. 6).

Рис. 6. Ключевые критерии выбора ЦОДа для клиента ▼

Источник: iKS-Consulting

Показательный пример того, что тариф не является определяющим фактором для большинства клиентов, приводит В. Железнов. В ЦОДе «Удомля» (Тверская область) стоимость электроэнергии составляет примерно 65–75% ее стоимости в Москве, что наряду с высокой экономической эффективностью объекта за счет его масштаба позволяет обеспечить тарифы на colocation примерно на 30% ниже, чем в столице, при точно таких же технических условиях. Хотя ЦОД в Удомле заполняется в соответствии с прогнозными показателями, резерв по вводу новых залов существенен – особенно на фоне периодического дефицита мощностей в Москве. «В значительной степени это объясняется психологическим фактором – это первый проект такого масштаба за пределами столицы, и при идентичных технологических и сервисных параметрах часть клиентов по-прежнему предпочитает размещение в Москве, несмотря на более высокие тарифы», – поясняет В. Железнов.

Получается, что, хотя цена электроэнергии чрезвычайно важна для конкуренции российских ЦОДов на мировом рынке, для клиентов ЦОДов в России она не критична. Куда важнее рассмотренные выше проблемы, связанные с большими временными и финансовыми затратами на технологическое подключение и масштабирование мощности.

До решения далеко, но диалог начался

Теперь немного официальной хроники. На совещании с Президентом РФ 10 июня 2020 г. представители ИТ-отрасли донесли до него проблемы, связанные с энергоснабжением ЦОДов. По итогам совещания президент поручил Правительству РФ проработать вопросы, касающиеся «предоставления организациям, являющимся операторами центров обработки данных, льготного доступа на рынок электрической энергии и мощности» (поручение № 1068 от 3 июля 2020 г.). Во исполнение данного поручения Минкомсвязь (ныне – Минцифры) России подготовила проект постановления правительства о внесении изменений в некоторые акты правительства в части предоставления ЦОДам такого доступа.

В проекте содержалось несколько предложений, в частности:

- определить особый порядок выполнения технологических подключений ЦОДов к электрическим сетям;
- снизить пороговые значения для работы ЦОДов на оптовом рынке электрической энергии и мощности;

● отнести ЦОДы к категории неотключаемых потребителей (ограничение режима потребления которых может привести к неблагоприятным экономическим, экологическим, социальным последствиям).

Однако Минэнерго России раскритиковало этот проект, указав, что ряд его предложений противоречит Федеральному закону «Об электроэнергетике», а их реализация может привести к сокращению конкурентного рынка электроэнергии, выручки генерирующих компаний, повышению тарифов для прочих потребителей и т.д.

Сейчас начат диалог между представителями Минцифры и индустрии ЦОДов, с одной стороны, и представителями Минэнерго и энергетиками – с другой, в том числе в рамках созданной рабочей группы по вопросам оптимизации энергоснабжения центров обработки и хранения данных. Одним из ключевых участников этого диалога является АНО КС ЦОД, выражающая точку зрения большинства игроков рынка коммерческих дата-центров.

«Мы сконцентрировались на двух направлениях работы, связанных с организацией технологических присоединений и резервированием мощности, поскольку считаем их наиболее важными для развития отрасли и обеспечения надежного функционирования ЦОДов», – рассказывает Дмитрий Бедердинов, генеральный директор АНО КС ЦОД.

Одна из поддержанных АНО КС ЦОД инициатив заключается в предоставлении дата-центрам возможности технологического присоединения одновременно к сетям нескольких сетевых организаций. Сегодня, если на земельном участке, где располагается ЦОД, имеется технологическое присоединение к одной сетевой организации, то он не может осуществить обычное технологическое присоединение к другой организации, даже в том случае, когда техническая возможность увеличения мощности отсутствует, а присоединение по индивидуальному проекту настолько экономически необоснованно, что от расширения ЦОДа приходится отказаться вообще. К сожалению, сложившаяся на данный момент практика именно такова.

Важно и то, что наличие альтернативного источника электропитания повышает надежность подключения к энергосистеме, а при присоединении к сетям нескольких сетевых организаций ЦОД в ряде случаев может обеспечить необходимый уровень надежности без устройств резервной генерации для ситуаций аварийного отключения.

Другая инициатива связана с возможностью компенсации ЦОДам затрат на строительство подстанций и других элементов энергетической инфраструктуры при подключении по индивидуальным проектам. Как упоминалось выше, расходы на такие объекты могут существенно превосходить обычную стоимость технологического присоединения. Не говоря уже о том, что в этих случаях создаются основные средства сетевой компании (коммерческой организации), с помощью которых она зарабатывает, поставляя энергию потребителю.

Третья инициатива касалась оплаты резервируемой мощности ЦОДа. Планируя переход на 100%-ную оплату резервируемой мощности, энергетики предполагали освободить от нее тех потребителей, кто подал заявку до определенного срока. Такая дифференциация давала преимущество ЦОДам, которые подали заявку ранее, и снижала конкурентоспособность вновь вводимых объектов. АНО КС ЦОД предложила ввести единые правила оплаты резервируемой мощности, при которых плата взимается только в случае, если выбрано менее 60% мощности, без разделения по срокам подачи заявки. Этот вопрос удалось урегулировать, и в новых готовящихся в Минэнерго правилах дифференциация объектов по срокам заявки не предусмотрена.

«В качестве позитивного момента отмечу сам факт начала диалога между энергетиками и ЦОДами. Мы пытаемся донести проблемы отрасли в части доступа к электроэнергии и, надеюсь, что мы придем к согласованным позициям, – продолжает Д. Бедердинов. – В конечном счете мы все заинтересованы в решении стратегической задачи повышения конкурентоспособности России, что невозможно без развития цифровой инфраструктуры».

«Российскому регулятору следует оценить ситуацию и предложить взаимовыгодные решения для квалифицированных энергоемких потребителей, представляющих стратегический интерес для страны с точки зрения ликвидации технологического отставания, которое пока – увы – только нарастает», – отмечает Василий Савин, руководитель практики KPMG по работе с компаниями сектора энергетики и коммунального хозяйства в России и СНГ.

Доступность электроэнергии всегда считалась важным конкурентным преимуществом России, но кратное превышение европейских показателей по временны́м и финансовым расходам на подключение к электросетям, а также фактическое отсутствие выигрыша по стоимости электроэнергии привели к тому, что отрасль ЦОДов потеряла это преимущество. Рост спроса на цифровые сервисы, конечно, обеспечит внутреннее развитие отрасли и в текущих энергетических условиях, но без их изменения о конкуренции на мировом рынке стоит забыть. ИКС

Проект ЦОДа: оптимальный результат в заданных финансовых условиях

Выбор площадки для ЦОДа и его проектирование – ключевые этапы, определяющие успех всего проекта. Опытом делится Евгений Вирцер, генеральный директор компании «Свободные Технологии Инжиниринг».

– Давайте начнем с выбора площадки. В России предпочитают строить ЦОДы в крупных городах, со всеми известными проблемами, в том числе связанными с дефицитом электроэнергии. Может быть, правильнее строить там, где она в избытке, например, рядом с электростанциями?

– Доступность электроэнергии – безусловно, важный фактор при выборе места для строительства ЦОДа, но далеко не единственный. Не менее важны другие параметры, в первую очередь качественная связь и транспортная доступность. Я пока не видел ни одного по-настоящему успешного коммерческого ЦОДа, построенного вдали от крупных городов в угоду близости к источникам дешевой электроэнергии.

– Но ведь такое размещение может упростить технологическое присоединение к электросети, которое становится настоящей головной болью для многих столичных проектов.

– Да, у нас в стране подключение к электросети занимает больше времени и требует больше денег, чем в Европе. И это не очень хорошо. Но практика показывает, что есть профессионалы, которые умеют решать такие задачи достаточно быстро и эффективно. Если люди занимаются этими вопросами постоянно, то у них нарабатывается необходимый опыт и экспертиза, которые позволяют оперативно подключить объект. Конечно, если компания занимается подключением первый или второй раз в жизни, например, строя по одному ЦОДу в пять-семь лет, то есть риск, как говорится, наступить на все грабли.

– Если взять три критерия выбора площадки – близость к клиентам, качественная связь и доступность электроэнергии, – как бы вы расставили приоритеты?

– Идеально, чтобы площадка была рядом с офисами большинства клиентов, источником дешевого электричества и узлами подключения нескольких десятков операторов связи. Но в жизни так не бывает. Если пришлось бы жертвовать чем-либо одним, то я бы выбрал стоимость энергии. Пусть электроэнергия обойдется дороже, но на площадку будет удобно заходить клиентам, и там будет хорошая связь.

Скажу так: если есть площадка, где электричество по 5 руб. за 1 кВт·ч, но там хорошая оптика и место удобно для клиентов, я бы выбрал ее, а не площадку, где электричество по 3,5 руб., но нет нормального подключения и она далеко от клиентов.

– Часто высказывается мнение, что ЦОДы выгоднее строить в холодных регионах, где есть возможность по максимуму использовать фрикулинг. Насколько климат влияет на выбор места для строительства ЦОДа?

– На мой взгляд, выбор холодного региона для строительства ЦОДа – еще не ключ к успеху. Для успешного функционирования ЦОДа важны десятки параметров в комплексе, основные из которых мы уже обсудили. Локация с удачными климатическими параметрами может не иметь нормальной энергетики и связи, возможностей для размещения специалистов и т.д.

– В мире много примеров экзотических мест размещения ЦОДов: в бывших шахтах, под водой, на воде… Насколько такие проекты вообще целесообразны или это в основном пиар?

– На мой взгляд, конечно, пиар. По аналогии с автомобилями – есть сногсшибательные штучные экземпляры, но для максимально эффективного и комфортного перемещения из точки А в точку Б люди все-таки используют серийные автомобили.

– Давайте поговорим о региональных ЦОДах. При каких условиях имеет смысл строить такие ЦОДы? Каковы могут быть меры поддержки местных властей?

– Я считаю, что ЦОДы в регионах строить необходимо, у них большое будущее. Но сегодня сначала должен появиться продукт, а уже за ним придет спрос. Поддержка региональных властей может выражаться в ускорении получения всех необходимых разрешений на строительство, СТУ, ну и, конечно, в том, чтобы помочь заполнить ЦОД клиентами (государственными компаниями и учреждениями).

Регионы с некоторой задержкой копируют то, что происходит в столице и крупных городах. Вспомните, когда лет 15 назад в Москве начинали строить первые коммерческие ЦОДы, ярко выраженного спроса не было, но объекты появлялись и довольно быстро заполнялись. Сначала нужен качественный продукт, который сформирует и раскроет спрос.

– Сегодня, в том числе для регионов, важна гибкость проекта, возможность наращивать емкость ЦОДа по мере необходимости. На что следует обратить внимание?

– При проектировании и строительстве ЦОДа этапами нужно правильно выбрать «квант» мощности модуля. В та-

ком случае можно будет максимально широко применять все существующие технологии, что даст ту самую гибкость и возможность масштабировать ЦОД оптимальным образом.

– Часто размером такого «кванта» называют 200 стоек.

– Мне нравится это число. 200 стоек по 5 кВт – для такого проекта имеется множество технических вариантов, большой выбор типового оборудования, всегда можно найти оптимальное решение, в том числе по цене.

Но возможны и другие «кванты». Например, мы сейчас проектируем несколько региональных ЦОДов с наращиванием по 50 стоек и максимальной емкостью 200 стоек – для этих регионов такой емкости пока достаточно. Универсального рецепта здесь нет.

– А edge-ЦОДы? Как обеспечить высокую надежность малых ЦОДов без больших затрат? Это вообще возможно?

– Чудес не бывает. Нет решений для малых ЦОДов, которые бы были надежны, как Tier III, но стоили бы, как Tier I. Да и в целом, не столь важен размер ЦОДа, сколь то, какие требования к надежности предъявляет его «начинка» – ИТ-оборудование и сервисы, которые на нем работают. Если системы, которые «крутятся» в ЦОДе, позволяют пойти на компромисс по надежности, то можно построить недорого. Если требуется уровень Tier III – надо быть готовым к соответствующим тратам.

Для edge-ЦОДов часто оптимально использовать модульные решения высокой заводской готовности – так называемые префабы. Главные преимущества этих решений – скорость и качество выполнения проекта. Можно уйти от индивидуального проектирования, от оформления разрешений на строительство и т.д., за несколько месяцев получив готовый продукт.

– Вы упомянули уровень Tier III. Но сейчас в России реализуются сразу несколько проектов Tier IV. Почему именно сейчас?

– Еще несколько лет назад считалось, что ЦОД Tier IV стоит значительно дороже, чем объект Tier III. Но накапливалась экспертиза, развивались технические решения, и вот специалисты нашли возможность реализовать требования Tier IV без существенного увеличения капитальных затрат. При этом в России ЦОДов Tier IV пока нет, а значит, построив такой объект и предложив услуги на его базе, оператор получит конкурентные преимущества. Совпадение этих факторов и определило начало практической реализации проектов Tier IV.

– Tier IV – это высокая отказоустойчивость. Что важнее для ее обеспечения: продуманность архитектуры, качество технических решений или эффективность службы эксплуатации?

– Основополагающей является совокупность названных факторов. Но если вы заставите меня выбирать один из трех, я выберу эксплуатацию. Плохая эксплуатация «убивает» все преимущества грамотной архитектуры и лучших технологий. А за счет правильной эксплуатации можно нивелировать небольшие огрехи, допущенные на этапах проектирования и строительства. Но подчеркну, именно небольшие, – средние и серьезные упущения на этих этапах уже никакой эксплуатацией не выправишь.

– В деле повышения эффективности эксплуатации, снижения вероятности ошибок, связанных с человеческим фактором, важна автоматизация. Увидим ли мы в ближайшем будущем полностью автоматизированные ЦОДы, для эксплуатации которых люди не нужны?

– Уровень автоматизации неизменно растет. Это очевидный тренд. Возможны ли полностью автоматизированные ЦОДы? Приведу пример из другой области. В Японии сделали полностью автоматические поезда метро. Но по просьбам пассажиров машинистов через некоторое время вернули. Людям оказалось психологически некомфортно ехать в поезде, в кабине которого никого нет.

Большинство процессов в ЦОДах со временем будет автоматизировано. Но без человека, считаю, не обойтись ни сегодня, ни завтра.

– Как правильно выбрать проектировщика будущего ЦОДа? Какими компетенциями он должен обладать?

– Основные системы ЦОДа, сильно влияющие на капитальные затраты и операционные расходы, – это энергетика и климат. Соответственно проектировщик должен обладать глубокими компетенциями как минимум в этих дисциплинах, а желательно и в других областях – автоматизации, пожарной безопасности и т.д. Идеально иметь в штате специалистов с глубоким предметным опытом работы именно в области ЦОДов, причем и коммерческих, и корпоративных.

Современные ЦОДы характеризуются большим числом пересечений различных инженерных систем. Проектировщик должен понимать их взаимозависимости – то, как малейшие изменения в одной системе могут влиять на другие, и т.п. Чем больше экспертизы у проектировщика, тем больше шансов, что все системы в совокупности будут работать должным образом.

Скажем, при проектировании жилых объектов часто привлекают специалистов извне, в том числе работающих на фрилансе. Каждый проектирует свою часть, а потом все сводится воедино, и получается хороший проект. С ЦОДами так не получится. Если проектировать разные системы по отдельности, стройного результата не будет.

Важно использовать современные цифровые инструменты, такие как BIM. Проектирование ЦОДа без применения BIM-технологий, конечно, возможно. Но подобный подход обычно приводит к большому количеству коллизий на этапе реализации проекта и, как следствие, к потере времени и денег. Что в итоге снижает конкурентоспособность конечного продукта.

Проектировщик ЦОДа должен уметь проектировать необходимый продукт в заданных финансовых условиях – а сегодня это большая редкость. Он должен уметь ставить под сомнение любое свое решение и всегда стремиться улучшить свой продукт, искать новые возможности, новые схемы, по сути быть на передовой технического прогресса в области цодостроения.

«Умная» локализация как драйвер цифровых инноваций для российской промышленности

Сергей Соловьёв, руководитель Центра компетенций, департамент «Цифровое производство», Siemens

Синергия российских разработок и передовых мировых технологий при создании промышленных цифровых решений – необходимая основа и залог обеспечения как уникальности и конкурентоспособности самих решений, так и эффективности их применения.

Развитие цифровых технологий и цифровая трансформация занимают важное место в актуальной российской повестке – и на уровне государственной политики, и в бизнес-стратегиях и текущих проектах компаний и корпораций. На оба процесса существенно влияют вопросы локализации и импортозамещения, причем это влияние распространяется не только на выпуск собственно промышленной продукции, но и на сферу программного обеспечения и шире – на цифровые технологии в целом. Попробуем взглянуть на некоторые особенности промышленных цифровых технологий как объекта локализации, попытаемся выявить наиболее критичные с точки зрения локализации компоненты и определить целевой подход к созданию российских цифровых решений.

Взаимопроникновение технологий: от зависимости к синергии

Информационные технологии как предтеча и основа цифровых технологий в их сегодняшнем понимании развивались и достигли высокого уровня как за счет прорывных инноваций в электронике, коммуникациях, цифровой обработке информации, создании программного обеспечения (ПО), так и благодаря взаимопроникновению решений, их комплексированию и обогащению дальнейшими разработками, а также благодаря принципам совместимости и открытости. Еще более серьезную роль взаимопроникновение, совместимость и комплементарность технологий играют в мире «цифры» сегодня: уровень комплексности и многосвязности технологического стека цифровых решений делает «цифровую совместимость» и использование готовых интегрируемых компонентов обязательными предпосылками для жизнеспособности цифрового продукта или услуги. При этом в экономической парадигме цифрового производства и цифровых моделей потребления такие связи между компонентами должны формироваться на лету для единичной кооперационной цепочки.

Мир цифровых технологий носит глобальный характер, несмотря на ряд существующих ограничений, и в силу этой его особенности, а также за счет региональной диверсификации технологических инноваций риск критической зависимости при использовании современных цифровых технологий все больше вытесняется риском неконкурентоспособности продукта или услуги. Есть также опасность, что из-за отсутствия опоры на доступные инструменты с подтвержденной эффективностью или из-за неиспользования синергии различных цифровых решений предприятие не сможет включиться в цифровые кооперационные цепочки.

Платформы и экосистемы – «среда обитания» цифровых решений

Арсенал цифровых инструментов и решений постоянно расширяется, и эта тенденция сохранится: она подкрепляется, с одной стороны, многообразием практических задач и сценариев применения, а с другой стороны – развитием самих технологий, обеспечивающих возможность повышения уровня комплексности и расширения спектра обрабатываемой информации, увеличения глубины обработки данных и эффективности извлечения бизнес-ценности. С учетом этой тенденции естественной и благоприятной жизненной средой для цифровых решений и инструментов стали платформы и экосистемы, способные предоставить необходимые условия для их создания, использования и развития. В числе прочего они могут решать задачи обеспечения производительности, масштабируемости, тира-

жируемости, информационной безопасности, вертикальной и горизонтальной интеграции, выполнять такие рутинные, но важные функции, как администрирование, обновление, балансировка нагрузки и т.п. В платформенно-экосистемном подходе к развитию цифровых решений всегда присутствует модель коммерциализации – т.е. фактически механизм, позволяющий как зрелой компании, так и креативному стартапу вывести на рынок и превратить в действующий бизнес собственные компетенции и разработки. Проприетарные решения и закрытые системы, даже передовые в своих сегментах, как правило, не способны обеспечить подобное сочетание технических возможностей и гибкой модели использования, в то время как платформенный подход снижает стоимость и сроки создания продукта или запуска сервиса, а наличие экосистемы позволяет обогащать решение и бизнес-цепочку новыми возможностями и кооперационными связями, получить гибкость в модификации алгоритмов, перестройке способов интеграции данных и создания новой ценности на их основе. Более того, востребованные специализированные решения или уникальные, но закрытые разработки могут обрести новую жизнь в качестве решений на базе цифровой платформы или сервисов в рамках цифровой экосистемы.

«Умная» локализация – создание высокотехнологичной добавленной стоимости

Создание цифровых решений в российских условиях связано с преодолением двух вызовов: технологического – получения доступа к передовому технологическому базису и нормативного – обеспечения соответствия предъявляемым корпоративным и законодательным требованиям. Несмотря на то что нормативная база в области цифровых технологий находится в процессе становления, действующие нормативные акты уже оказывают существенное влияние на формирование ландшафта цифровых решений и векторы дальнейшего развития российской индустрии цифровых продуктов и сервисов.

Можно выделить следующие важные ниши для применения передовых мировых технологий в российской промышленности:

- создание отраслевых платформенных решений, обеспечивающих построение интегрированного цифрового производственного контура предприятия;
- формирование экосистем цифрового взаимодействия участников производственной цепочки и компаний – провайдеров комплексных цифровых сервисов.

В рамках платформ и экосистем могут быть реализованы различные универсальные и специализированные системы и сервисы: от удаленного мониторинга, поддержки принятия решений, предиктивной аналитики, прослеживаемости до интеграции производственных систем с системами ERP, BI, S&OP и др. – на основе как локальной, так и облачной инфраструктуры.

Следование принципам локализации подразумевает, что ключевая составляющая, определяющая функциональность и бизнес-ценность таких решений, формируется в виде результата интеллектуальной деятельности российских компаний. При этом цель создания и применения цифровых систем и сервисов остается неизменной во всех цифровых юрисдикциях, в том числе российской: это создание высокотехнологичной добавленной стоимости на всех этапах жизненного цикла промышленной продукции за счет новых бизнес-моделей. Таким образом, чтобы получить ощутимый бизнес-эффект в короткие сроки, в первую очередь нужно реализовать развитый функционал, обе-

спечивающий всеобъемлющую интеграцию в рамках производственных систем и сквозных бизнес-цепочек. В этой связи синергия российских разработок и передовых мировых технологий при создании промышленных цифровых решений видится необходимой основой и залогом обеспечения как конкурентоспособности самих решений, так и эффективности их применения.

Обеспечить безопасность

Одновременно на новый уровень выходят вопросы кибербезопасности – соответствующие технические решения, очевидно, обязательны для любого современного цифрового продукта или системы. Учитывая скорость развития цифровых систем и решений в промышленности, а также динамический характер связей и транзакций в цифровой парадигме, объектом внимания и предметом защиты здесь стали не только сами системы, но и процессы их создания и использования.

Адекватные подходы к кибербезопасности в условиях глобального взаимопроникновения информационно-коммуникационных технологий и их массовой интеграции в производство вырабатываются на основе лучших мировых практик и гармонизации стандартов (в частности, стоит упомянуть выпуск российских стандартов группы МЭК 62443) – безусловно, с учетом специфических российских требований и действующей нормативной базы. В целом усиление нормативного регулирования и ужесточение корпоративных стандартов способствуют повышению зрелости решений и подходов к обеспечению кибербезопасности.

Развитие цифровой экспертизы России: инженерный и научно-технический потенциал в действии

Целям российских компаний, разрабатывающих приложения и OEM-решения, в наибольшей степени соответствует платформенно-экосистемный подход. За счет использования развитого инструментария и функционала «из коробки», доступных, например, в качестве готовых сервисов или библиотек, компании могут сосредоточиться на реализации прикладной бизнес-логики и отличительной добавленной ценности продукта. При этом могут быть существенно сокращены сроки реализации и вывода на рынок собственных разработок – а быстрота создания и модификации относится к числу ключевых факторов для цифровых решений.

Опора на доступные на рынке компоненты и сервисы при ориентации на лидирующие, активно развивающиеся отраслевые стандарты и технологии на практике не повышает, а снижает риски технологической зависимости, поскольку обеспечивает возможность модификации или миграции на альтернативные компоненты или решения (в том числе на основе открытого исходного кода) без существенных затрат времени, а самое главное – без потери непрерывности бизнеса. Это выгодно отличает такие решения от закрытых или полностью «самописных» как в плане достижимого уровня качества и функциональности, так и с точки зрения дальнейшего развития и сопровождения.

Еще более значима для локализации возможность задействовать колоссальный потенциал, накопленный отечественной наукой и инженерной школой, в сфере математического (в том числе имитационного) моделирования различных технологических процессов и производственных систем. Говоря сегодняшним языком – в сфере цифровых двойников, которые становятся частью современных киберфизических систем. Использование этого научно-инженерного аппарата в составе российских решений для цифровизации производства позволяет не только обогатить их развитым функционалом, но и обеспечить рыночную уникальность – как на локальном, так и на глобальных рынках.

В качестве примеров действенности такого подхода к локализации можно привести OEM-решения для энергетики, нефтегазового секто-

ра, инфраструктуры, реализованные российскими компаниями. В этих областях уже есть практические результаты – причем не только в виде готовых программных продуктов, но и в виде реальных производственных активов, охваченных сервисами на базе данных программных решений.

Госкорпорации: цифровой суверенитет и критическая информационная инфраструктура

Говоря о локализации цифровых решений, нельзя обойти стороной тему создания и внедрения решений для госкорпораций, поскольку они стали не только ключевыми контрибьюторами российской экономики, но и активными участниками цифровой трансформации. При этом госкорпорации выступают и как компании – потребители цифровых продуктов и услуг, и как организации и даже органы, определяющие подходы, приоритеты, архитектуру и стратегии цифровой трансформации.

Одно из ключевых требований для госкомпаний и госкорпораций – обеспечение «цифрового суверенитета»: сюда относятся локальное хранение бизнес-критических, технологических и других данных, выполнение требований информационной безопасности, приоритет использования российского ПО и информационно-телекоммуникационной инфраструктуры. Существенно влияют на формирование цифрового ландшафта госкомпаний и требования в отношении критической информационной инфраструктуры, определенные Федеральным законом № 187-ФЗ и соответствующими приказами ФСТЭК.

Примерами выполнения требований госкомпаний при создании прикладных систем на базе решений, апробированных мировым опытом применения, могут служить реализованные крупномасштабные проекты в российских государственных компаниях нефтегазового сектора, гидроэнергетики, транспортной инфраструктуры, в том числе на базе уже упоминавшихся решений. При их разработке учитывались как интересы заказчиков, так и технические требования к архитектуре, функциональности, визуализации, кибербезопасности, производительности и др.

Дальнейшая работа должна, по всей видимости, вестись в направлении обеспечения совместимости с отечественными операционными системами, СУБД и другим системным ПО, интеграции с корпоративными информационными системами и сервисами, включая упомянутые выше платформы. Очень важным шагом стало бы внесение таких решений в Единый реестр российских программ для электронных вычислительных машин и баз данных. Кроме того, существуют огромные возможности для развития облачной парадигмы, в том числе за счет развертывания частных облаков.

Экспортный потенциал и инклюзивное промышленное развитие

Помимо рассмотренных выше вызовов, развитие конкурентоспособных цифровых решений и высокотехнологичных сервисов важно и с точки зрения повышения экспортного потенциала российской промышленности. Синергия передовых мировых цифровых технологий и ведущих российских разработок способна обеспечить уникальность предложения компаний и корпораций, вовлеченных во внешнеэкономическую деятельность или стремящихся к экспансии на внешние рынки. Таким образом, экспортный аспект дает еще один довод в пользу прагматичного подхода к локализации с ориентацией на лучшие мировые практики и технологии и развития на их основе собственных высококонкурентных решений.

Важно подчеркнуть, что такие решения и сервисы относятся не только к уровню собственно производственных площадок, но охватывают всю экосистему кооперации – инжиниринговые, сервисные, ИТ-компании, компании-поставщики, участвующие в цикле разработки, производства и обслуживания промышленной продукции. Таким образом, формирование интегрированных производственных экосистем на базе цифровых технологий и решений не только способно обеспечить рост в отдельных сегментах и промышленности в целом, но и напрямую соответствует целям локализации – развитию локальных компетенций и созданию высокотехнологичного задела.

«Умная» локализация передовых цифровых технологий и развитие собственных инновационных решений на их основе – залог создания высокотехнологичной добавленной стоимости в России, а также продвижения конкурентных высокотехнологичных продуктов и услуг на внешние рынки. Все это позволит обеспечить устойчивое и инклюзивное развитие российской промышленности. ИКС

Рынок инженерной инфраструктуры ЦОДов устойчиво растет

Несмотря на сложные условия, компания Vertiv с оптимизмом смотрит в будущее. О том, как компании удалось добиться высоких результатов, – Николай Харитонов, глава представительства Vertiv в России и Беларуси.

– Николай, какие факторы влияют на рынок инженерной инфраструктуры ЦОДов?

– Цифровая трансформация, подстегнутая пандемией, приводит к проникновению компьютерных технологий во все сферы жизни. Широко используются онлайн-сервисы, дети учатся через интернет, люди общаются с помощью видеоконференций, компании переходят на удаленный режим работы.

Несмотря на экономический спад и приостановку многих бизнесов, массовый спрос на ИТ-услуги вызвал в первом полугодии рост продаж инженерной инфраструктуры для ЦОДов, ведь именно ЦОДы обеспечивают работу особенно востребованных в пандемию сервисов.

Еще один фактор – позиция государства, которая будет способствовать развитию рынка при реализации программы «Цифровая экономика РФ». Так что спрос на системы охлаждения и электропитания для дата-центров будет только увеличиваться.

– Каким стал этот год для Vertiv, какие планы удалось осуществить?

– С точки зрения рынка перспективы года выглядели пессимистично, ведь помимо эпидемии COVID-19 на экономическую ситуацию в России сильно повлияло снижение цен на нефть. Опыт показывает, что ИТ-бюджеты коррелируют со стоимостью нефти. Когда цена нефти растет, в России покупают и потребляют ИТ-продукты, внедряют масштабные инфраструктурные проекты. Когда падает – все сокращается и замирает. Мы ожидали, что будет тяжело, тем не менее за прошедшие три квартала компания Vertiv в России показала рост и даже перевыполнила планы. Причем планы составлялись осенью прошлого года, когда никто не мог предположить «заморозки» экономики на два-три месяца и затяжного падения цен на нефть.

– Первая волна эпидемии COVID-19 затронула многие страны. Повлияло ли это на выпуск продукции заводами Vertiv в разных странах мира и на поставку заказов?

– Когда СМИ начали передавать тревожные репортажи о росте заболеваемости и введении карантинных мер по всему миру, мы стали переживать по поводу возможных перебоев в поставках оборудования Vertiv в Россию. Однако карантин не повлиял на работу заводов Vertiv, продукция которых считается критически важной. Все меры предосторожности были приняты и контролировались на самом высоком уровне. Проблем у получателей не возникало – заказы выполнялись в срок, грузовая логистика работала, оборудование доставлялось в Россию. Ограничения касались только физических лиц, а товары свободно перемещались между странами.

– Какая продукция Vertiv пользуется спросом в России? С какими крупными компаниями работаете?

– Восемьдесят процентов деятельности Vertiv относится к проектному бизнесу – комплексным решениям для ЦОДов, как крупных коммерческих, так и средних корпоративных мощностью до сотни киловатт. Наши основные точки роста – коммерческие ЦОДы, предоставляющие услуги по модели colocation, и телеком-компании, чьи бизнес-интересы постепенно смещаются в сторону ИТ. Сейчас они активно вкладывают деньги в покупку или строительство дата-центров, а также в облачные технологии. Это ключевые отрасли для Vertiv, обеспечивающие рост на российском рынке. Если говорить о конкретных компаниях, то в России мы работаем с «Ростелекомом», IXcellerate, DataPro, O2xygen. В Беларуси мы построили модульный ЦОД для провайдера BeCloud. Выделить один продукт сложно, так как мы поставляем всю инфраструктуру. Стабильный рост показывает направление прецизионного охлаждения, год от года увеличиваются поставки источников бесперебойного питания, стоечного оборудования, PDU. На расширяющемся рынке ЦОДов мы растем даже быстрее рынка.

Также мы видим серьезный потенциал развития в сегменте рынка малых ИБП, защищающих рабочие станции и узлы автоматики. Несмотря на падение рынка однофазных источников бесперебойного питания в России, наша доля увеличива-

ется. Планируем и дальше инвестировать в развитие канала: внедрять новые опции в партнерскую программу, и, конечно, развивать продуктовое портфолио с фокусом на edge-решения.

– Как снизить количество эксплуатационного персонала в помещениях ЦОДа, что особенно важно в условиях карантинных мер и пандемии?

– При реализации проектов мы предлагаем систему мониторинга. Оператор ЦОДа может управлять ей в единой консоли, оперативно получая информацию о состоянии инженерных узлов, рекомендации по эксплуатации и уведомления о возможных аварийных ситуациях.

Полностью отказаться от персонала в ЦОДе невозможно. Должны быть смены, контролирующие состояние оборудования и реагирующие на штатные и нештатные ситуации. Но можно оптимизировать число сотрудников и перевести на удаленный режим некоторых специалистов, например, тех, кто отслеживает работу ИТ-сервисов, дистанционно запускает серверы и переустанавливает ПО.

Компания Vertiv предоставляет дата-центрам услуги мониторинга и анализа состояния инженерного оборудования Vertiv LIFE Services. Оператор центра предиктивной аналитики компании Vertiv отслеживает тысячи локаций и в случае проблем предлагает клиентам перезапустить оборудование, установить новое программное обеспечение, а заранее предположив возможный выход из строя – заменить узел или батарею. Это позволяет компаниям сократить штат службы эксплуатации, повысить эффективность работы.

В России рынок еще не готов отдавать подобную работу на аутсорсинг. Есть опасения в отношении безопасности и возможных репутационных рисков, ведь ЦОДы «продают» надежность и не всегда хотят огласки возникающих проблем. В России системы мониторинга Vertiv успешно внедряются, но на уровне служб эксплуатации дата-центров в закрытых сетях.

– Какими сертификатами чаще всего интересуются заказчики?

– Все поставляемое в Россию оборудование соответствует российским ГОСТам и Правилам устройства электроустановок Госэнергонадзора. Часто наши заказчики интересуются сертификацией Eurovent Certita Certification. Ассоциация Eurovent – один из основных органов европейской сертификации климатического и холодильного оборудования. Именно она определяет, насколько оборудование соответствует заявленным параметрам. Энергоэффективность подтверждает международный стандарт Energy Star.

В последнее время компания стала сертифицировать готовые модули заводской готовности для дата-центров по стандарту Tier Ready. Мы разрабатываем дизайн модуля: как будет расположено оборудование, какие используются ИБП, системы охлаждения, пожаротушения, и согласовываем его с Uptime Institute. Получается типовой готовый продукт заводской готовности, который можно выбрать в нашем портфолио. Соответствие требованиям популярного в России Uptime Institute свидетельствует об уровне надежности, о том, что время простоя дата-центра в течение года не превысит определенного значения.

– Как обеспечить высокие требования надежности в edge-ЦОДах при минимизации затрат?

– Edge-ЦОД – небольшой вычислительный кластер для оперативной обработки информации на периферии сети: в филиале, цехе, магазине. Его надежность не менее важна. Ведь перебои в работе могут повлечь за собой сбои в бизнес-процессах и грозить репутационными рисками, что особенно критично для сервисов. У компаний бывает искушение установить для пары стоек и бытовой кондиционер. Какое-то время он будет работать. Но специализированное сертифицированное оборудование проработает дольше, его энергоэффективность будет выше, а совокупная стоимость владения ниже.

Не стоит экономить за счет интеграции нового оборудования с элементами уже имеющейся старой инженерной инфраструктуры, снижающей надежность решения в целом. Эффективнее использовать наши отработанные интегрированные решения для филиальных сетей разных уровней надежности: от филиальной сети банка до распределенной сети туристических агентств. Такие решения включают возможность удаленного управления и мониторинга. Ведь нет смысла в каждой точке держать ИТ-специалиста.

– Какое влияние на бизнес компании в России оказывают процессы импортозамещения?

– Мы следим за процессами импортозамещения, изучаем возможности изготовления оборудования на российских заводах, но в ближайшей перспективе, в 2021 г., к локализации производства и открытию своего завода в России не готовы. Рынок сбыта не соответствует требуемым инвестициям. Да и крупных заводов, выпускающих специализированное климатическое оборудование, в стране нет. Тем не менее мы идем навстречу российским производителям, желающим работать с нашим оборудованием, которое поставляется в OEM-формате.

– Каковы планы Vertiv по развитию бизнеса в России?

– Мы активно развиваем канальное направление и наблюдаем рост в этом сегменте. В этом году заключили соглашение с новым крупным российским дистрибьютором – компанией Treolan. Усовершенствовали партнерскую программу, упростили регистрацию новых партнеров, запустили новый портал – теперь партнеры видят свои бонусы, сертификаты, могут регистрировать сделки и проходить обучение онлайн. Продолжим развитие SMB-формата, сотрудничество с небольшими реселлерами, продающими маленькие ИБП. Будем наращивать количество партнеров, стремиться к тому, чтобы им было удобнее и выгоднее работать с компанией Vertiv.

Планируем дальнейшее развитие направления дата-центров, увеличение числа менеджеров отдела продаж. В приоритете – коммерческие ЦОДы, телеком, банки, страховые компании и нефтегазовая отрасль.

Экосистемных окон негасимый свет

Константин Рензяев, генеральный директор, CorpSoft24

Одним из важных трендов развития экономики эксперты называют создание экосистем – тесно связанных между собой сервисов, работающих по принципу «одного окна».

Предположения о том, что через несколько лет во всех сферах останутся только Сбербанк, «Ростех» и «Яндекс», раньше воспринимались как сарказм. Но сегодня, с учетом возможностей облаков, экосистем и объединенных точек доступа к ним, ироническая составляющая таких высказываний становится все меньше.

Сегодня компании во многих отраслях стремятся взять на себя роль многопрофильного центра, предлагающего целый набор готовых решений. Появляются экосистемы разнородных сервисов и продуктов, предоставляемых одним провайдером в формате «одного окна» за счет расширения собственного портфеля компетенций либо через партнеров.

ИТ, телеком и банки – в лидерах

Яркие примеры реализации экосистемного подхода с доступом к портфелю сервисов и продуктов через одно окно – банковский сектор и телеком. Предложения Сбербанка, Тинькофф, ряда операторов связи, в частности МТС (который сегодня уже не просто оператор связи, но и банк и облачный провайдер), отлично иллюстрируют данный тренд. Безусловный российский лидер в этом направлении – «Яндекс». Компания недавно зарегистрировала несколько доменов, в том числе под банковскую деятельность. Стремительно развивается Сбербанк: если в начале 2019 г. его экосистема насчитывала 20 компаний, то всего за год в нее удалось вовлечь еще 28 проектов. При этом за два года банк потратил на построение своей экосистемы 125 млрд руб.

На глобальном рынке самые дорогие и быстрорастущие компании – многопрофильные ИТ-игроки. В топ-5 самых богатых бизнесменов планеты входит лишь один не «цифровой» представитель – владелец Louis Vuitton Бернар Арно.

В перспективе экосистемный подход одинаково выигрышен для всех отраслей. Можно строить полноценные B2B-экосистемы с последующей интеграцией продуктов их работы в B2C-экосистемы. Даже вокруг сельхозсектора появляются инновационные компании, предоставляющие, скажем, услуги управления техникой, анализа урожайности на основе технологий больших данных и искусственного интеллекта и т.д. Менее всего подобные тенденции заметны на предприятиях машиностроения, что обусловлено большим объемом требуемых инвестиций как в основное производство, так и в ИТ, необходимые для качественного цифрового рывка.

Почему и как это работает

В экосистеме синергический эффект увеличивается по мере роста числа участников и повышения уровня их вовлеченности. Формируется большое разнообразие продуктов/услуг в едином центре доступа в рамках объединенного предложения.

Формат одного окна и экосистемы тесно связаны между собой. Можно сказать, что любая экосистема продуктов и сервисов стремится достичь в своем развитии формата одного окна для клиентов. Для этого сначала должна сформироваться единая точка выхода в виде продуктового предложения: веб-портал, help desk, приложение, где по запросу доступны все необходимые возможности сервисов, решений и технической поддержки. Затем предложение расширяется, унифицируется, и для доступа к нему создается единый интерфейс.

Первоначально экосистемы сервисов и продуктов формировались эволюционно: провайдер постепенно набирал компетенции в своей отрасли и выводил на рынок новые предложения. Каждое направление развивалось обособ-

ленно, но в какой-то момент их разрозненные системы service desk объединялись, и таким образом экосистема сервисов приобретала формат одного окна. Сегодня мы видим расцвет коммерческого пути создания экосистем: компании-гиганты скупают готовые продукты и сервисы, включая приобретения в свой пул предложений. Конечно, эволюционный способ продолжает работать, особенно в крупных экосистемах, где компании с помощью своих R&D-отделов на основе общей технологической базы запускают собственные разработки, которые встраиваются в систему одного окна.

Экосистемы + облако = бизнес будущего?

Одна из причин популярности экосистем – развитие облачных платформ и предоставляемых ими возможностей. Привязка к облакам – технологическая, вызванная более общей тенденцией к использованию платформ в качестве стандарта для множества актуальных бизнес-задач. Платформы облегчают интеграцию продуктов и сервисов между собой, обеспечивают отказоустойчивость и упрощают доступ к ресурсам экосистемы.

Сегодня практически любое программное решение, лежащее в основе современных сервисов, разворачивается на облачной платформе как на оптимальном инфраструктурном фундаменте бизнеса, к которому проще, дешевле и экономически целесообразнее «прикручивать» все остальные инструменты и функции. IaaS- и SaaS-решения, доступные в рамках облачных платформ, покрывают технологические потребности поддержки работы экосистемы и интерфейса одного окна в полном объеме. Как правило, достаточно стандартного набора ресурсов и архитектуры, а далее внутри арендованных ресурсов каждая компания настраивает детали необходимой для ее задач конфигурации.

В облаках развернуты open source-платформы service desk, например Open source Ticket Request System (OTRS), откуда любой провайдер может ее «достать», сконфигурировать нужным образом, использовать для себя в любых средах и даже оформить решение на базе OTRS под собственной лицензией для коммерческого распространения.

По нашему опыту, сегодня в облачной парадигме прекрасно реализуются сервисы, построенные вокруг программ автоматизации бизнеса. Для экосистемы в облаке подходят все сервисы и продукты, позволяющие бизнесу максимально «отторгнуть» от себя непрофильную деятельность и получить качественный сервис, не отвлекаясь от основной работы. При этом облако является фундаментом всей экосистемы.

Прорубить «одно ИТ-окно»

Основные сложности создания сервиса по принципу одного окна или экосистемы заключаются в распределении ролей и ответственности между партнерами, а также в организации ИТ-архитектуры. В теории все легко – команды специалистов вовлеченных в проект сторон переводятся на единую систему service desk, организуется служба диспетчеризации и работа запускается. Но на практике процесс идет не так гладко. Проблемы возникают при «притирке» команд каждого из направлений, потому что четко разграничить зоны ответственности невозможно.

В целом же переход к экосистемному мышлению ставит под сомнение унаследованную от промышленной революции саму идею «индустрии» как дискретного набора схожих конкурирующих между собой игроков, производящих однородный продукт вертикально интегрированным способом. В ближайшие десятилетия экосистемы, скорее всего, распространятся еще шире, и компании будут сосуществовать в кластерах, выходящих за рамки традиционных отраслевых границ.

В этом свете процесс построения эффективной экосистемы потребует умения правильно распознавать драйверы, которые могут способствовать синергическому эффекту. Определение правильных драйверов, в свою очередь, вытекает из общего видения целей участников экосистемы.

Риски и выгоды

Главный риск, наиболее высокоуровневый и наименее реалистичный, – «падение» бизнеса провайдера одного окна как такового. Он относится к форс-мажорным обстоятельствам глобального характера, от которых не застрахован полностью ни один игрок, даже самый крупный и защищенный. Рисков информационной безопасности в бизнес-модели одного окна значительно меньше, чем при получении того же набора сервисов и продуктов у нескольких разрозненных поставщиков.

Использование одного окна выгодно с экономической и операционной точек зрения. Когда клиент покупает у провайдера несколько услуг, к нему формируется более лояльное отношение. Также возникает возможность решать все текущие вопросы в единой зоне ответственности и точке диалога.

Следует помнить, что идеальных провайдеров всего спектра компонентов экосистемы нет, всегда существует риск отставания по какой-либо узкой компетенции. Например, 90% потребностей бизнеса текущие предложения экосистем закрывают, но для решения отдельных узкоспециальных задач лучше обращаться непосредственно к провайдеру соответствующего сервиса. ИКС

Спутниковый доступ необходим на 99% территории страны

За пределами мегаполисов «последняя миля», определяющая доступность и качество ИКТ-сервисов, часто реализуется только с помощью спутникового доступа. Об особенностях этого рынка – Александр Аносов, генеральный директор компании «Дозор-Телепорт».

– Александр, как в целом развивается сегодня сегмент спутниковой связи?

– Спутниковая связь показывает устойчивый рост, она является важной составной частью общего тренда на повсеместную цифровизацию, который мы наблюдаем в глобальных масштабах. По прогнозам NSR, темпы увеличения количества активных абонентов VSAT в ближайшие годы будут двузначными – до 25%! – во всех регионах мира, за исключением Северной Америки.

Рост спроса на спутниковую связь приводит к росту предложения и, как следствие, к снижению стоимости спутникового ресурса и повышению доступности данного сервиса. Так, по данным Euroconsult, объем аренды мощностей спутников для передачи данных увеличивается в среднем на 23% в год, и такой темп сохранится до 2028 г. Усиление конкуренции между владельцами спутников приведет к снижению стоимости спутникового ресурса к 2028 г. на 67% – с $585 до $191 за 1 Мбит/с в месяц.

– Давайте перейдем от глобальных трендов к российским реалиям. Какой процент российских пользователей нуждается в спутниковом доступе?

– Этот вопрос следует сформулировать немного по-другому: где российский абонент будет нуждаться в спутниковом доступе? Ответ: на 99% территории страны. Мегаполисы с городами-спутниками и другие крупные города имеют неплохую телекоммуникационную инфраструктуру, как кабельную, так и определяемую беспроводным покрытием. Но за пределами городов все выглядит несколько иначе – даже в Московской области много населенных пунктов, где широкополосное подключение лучше получать через спутник, а по наземным каналам обеспечить его непросто.

Конечно, в последние годы государство многое сделало для расширения проникновения широкополосного доступа в отдаленные города и поселки. Но чудес не бывает: никто не будет прокладывать оптоволокно в удаленную деревню из полусотни дворов, это экономически невыгодно. Поэтому на территории нашей огромной страны спутниковый доступ крайне актуален как для частных лиц, так и для корпоративных пользователей: предприятий, органов госуправления, объектов критической инфраструктуры и т.д.

В количестве подключений предсказуемо лидируют Дальневосточный и Сибирский федеральные округа, на которые приходится половина всех VSAT-станций в России. Они же показывают самые высокие темпы роста, например: в 2019 г. в них были установлены 46% новых VSAT-станций в стране. Но рост мы наблюдаем и в других регионах, например, по итогам 2019 г. в Уральском и Поволжском федеральных округах количество VSAT-станций увеличилось на 20%, а в Центральном – на 12%.

– Какова роль государства в развитии спутникового доступа?

– Спутниковый доступ активно используют для подключения социально значимых объектов в рамках федерального проекта «Информационная инфраструктура», развернутого в рамках национальной программы «Цифровая экономика РФ». Например, сейчас мы выполняем подключение к интернету более чем 1200 социальных структур в Республике Саха (Якутия). Это школы и учреждения среднего профессионального образования, фельдшерско-акушерские пункты, отделения полиции и Росгвардии, пожарные части, военкоматы, органы государственной власти и местного самоуправления. Соответствующий тендер «Дозор-Телепорт» выиграл в прошлом году, работы займут два года.

Также в рамках проекта «Информационная инфраструктура» к 2024 г. планируется создать спутниковую группировку связи «Экспресс-РВ» из пяти космических аппаратов, которые будут предоставлять услуги ШПД на всей территории России и в Арктике. Кроме того, действует федеральная целевая программа «Сфера», предполагающая развертывание в 2023–2028 гг. орбитальной группировки из более чем 600 спутников с высокой пропускной способностью, мощностей которых будет достаточно, чтобы одновременно обеспечивать связью до 10 тыс. подвижных объектов транспорта, такое же количество точек коллективного интернет-доступа и 10 млн абонентов персональной связи.

– Много ли в России предприятий расположено вдали от населенных областей, охваченных развитой проводной инфраструктурой?

– Много. Например, большая часть структур нефтедобывающей промышленности. И «нефтянка» – лишь один при-

мер вертикального рынка, который остро нуждается в спутниковой связи, пример наиболее яркий, но не единственный. Сюда же отнесем другие предприятия добывающей промышленности, лесозаготовку, энергетиков, транспорт, объекты дорожной инфраструктуры, федеральные торговые сети и т.д.

Напомню, что спутниковый доступ может быть как стационарным, так и мобильным. Мы можем обеспечить ШПД для яхт, прогулочных и транспортных судов, поездов, туристических автобусов, самолетов. Сегодня широкополосный доступ важен и для мобильных групп: экспедиций, сервисных бригад, аварийных команд и т.п.

Замечу, что спутниковый доступ актуален даже для тех предприятий в удаленных районах, которые имеют ШПД по кабельным каналам.

– Зачем таким компаниям «спутник», если у них есть наземные каналы?

– Для обеспечения непрерывности бизнеса. Наземные каналы большой протяженности по понятным причинам уязвимы для внешних воздействий, поэтому в качестве резервных сейчас все чаще используют спутниковые каналы. Случился очередной паводок, копали канаву или, например, перекладывали шпалы – вот и повреждено оптоволокно или затоплены короба с кабелями, без доступа в интернет остался город или даже несколько географически близких населенных пунктов. А в них работают сотни структур, которым без интернет-доступа сегодня проблематично или невозможно вести бизнес либо, если мы говорим о госструктурах, выполнять свои функции.

Технически избежать такой ситуации с использованием наземных структур можно – нужно лишь подвести резервный канал, удаленный от основного. Но тянуть оптоволокно на тысячи километров для резервирования экономически нерентабельно, да и неразумно – ведь спутниковый интернет доступен на всей территории страны. Кроме того, спутниковый канал не зависит от расстояния до подключаемого объекта, что выгодно отличает наши сервисы от кабельных.

– Вы выступаете и как провайдер, и как интегратор?

– В сегменте частных абонентов говорить об интеграции, наверное, не стоит – оборудование даже для коллективного использования канала коробочное. Но задачи корпоративных абонентов более разнообразны, поэтому тут при подключении от нас требуются функции консалтинга, а иногда и интегратора.

В нашей структуре – а мы входим в состав холдинга – есть профильное подразделение, которое способно решать задачи заказчиков в плане интеграции. За время существования мы наработали ряд интересных кейсов, имеем профильную экспертизу для многих вертикальных рынков, например, для упомянутой «нефтянки», для морских и речных судов, для энергетиков и т.д.

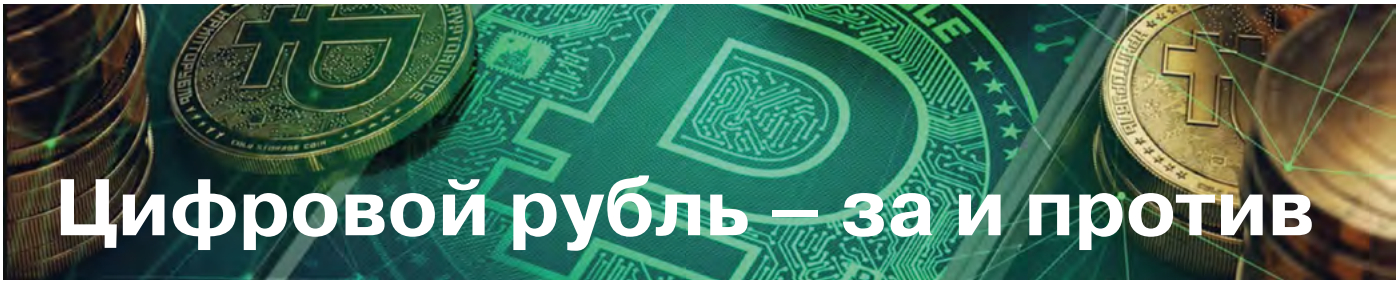
Задачи у заказчиков весьма разнообразные. На базе спутникового канала можно обеспечить практически все: передачу данных, телефонную связь, видеоконференции, видеонаблюдение, оперативно-диспетчерское управление и т.д. Согласитесь, что телеком-сервисы для M2M, для репликации баз данных, для телефонии или только для электронной почты должны быть немного разными, как в техническом плане, так и в плане экономики. Кроме спектра задач своеобразие вносит структура предприятия – наши заказчики часто имеют филиалы, распределенные по большой территории, которым иногда нужна связь с заданными параметрами для коммуникаций с центральным офисом, друг с другом, с удаленными серверами и т.д.

– Насколько «тесно» в сегменте операторов спутникового доступа?

– Ситуация в российском сегменте своеобразная: в стране есть два вертикально интегрированных оператора спутниковой связи – ФГУП «Космическая связь» и АО «Газпром космические системы», – располагающих собственной инфраструктурой: как спутниками, так и наземными станциями. Кроме того, работают несколько десятков виртуальных операторов, которые предоставляют услуги спутниковой связи на основе инфраструктур двух упомянутых операторов.

«Дозор-Телепорт» изначально являлся базовым оператором (HNO) – у нас свои центральные земные станции спутниковой связи, – но в дальнейшем стал применять также модель виртуального оператора (VNO), исходя из экономических предпосылок реализации определенных проектов. Сейчас мы поставляем услуги на разных платформах. Из используемых нами платформ 80% построены по модели HNO, что позволяет предоставлять услуги с высоким качеством сервиса. Но 20% задействуют модель VNO, что помогает нам конкурировать в низкомаржинальных проектах. Наша политика дает возможность не просто перепродавать услуги, а предоставлять более гибкие тарифы, обеспечивать дополнительные и сопутствующие сервисы, консалтинговые услуги и многое другое.

Как я уже говорил, российский рынок спутникового доступа растет. Основная причина – продолжающийся курс на интернетизацию всего, от бизнес-процессов до повседневной жизни. Также росту способствует заметное снижение цен на конечное оборудование. Мы видим неуклонную эволюцию в настоящем и потенциал для роста на перспективу. Как обычно, основную часть рынка контролируют топ-5 крупнейших игроков сегмента, к которым относимся и мы. «Дозор» давно присутствует в сегменте, у нас много лояльных абонентов, развитые каналы продвижения, техническая экспертиза, репутация. Это позволяет нам расти опережающими темпами и, как следствие, обгонять рынок.



Цифровой рубль – за и против

Николай Носов

Насколько целесообразно введение цифрового рубля, предложенного Банком России? Каковы могут быть модели его использования?

Зачем нужен цифровой рубль?

Мы все реже пользуемся наличными деньгами, прикладывая вместо этого к терминалу банковскую карту, переводя деньги со смартфонов или оплачивая товары и услуги через интернет. Безналичные деньги не рвутся, вор в трамвае не вытащит кошелек из кармана, а если украдет карту, то ее можно быстро заблокировать. В случае крупных покупок не надо носить чемодан с деньгами. Бизнесу удобнее вести учет расходов и доходов на компьютере, а не пересчитывать купюры в мешке. Не нужны бронированный сейф, платежи за инкассацию и вооруженная охрана для перевозки купюр. Безналичные расчеты вытесняют наличные, победу одерживает безналичный рубль.

Однако у наличных денег есть свои козыри, которые не дают завершить процесс цифровизации денежного оборота. Как популярно объяснил знакомый банкир, деньги клиента в банке – это уже деньги банка, а не деньги клиента. После внесения на счет, перевода наличных в безналичную форму клиент теряет над ними контроль в обмен на обязательства, которые финансовая организация может и не выполнить. Произойти это может не только в случае отзыва лицензии. Банк может задержать платеж из-за нехватки денег на корсчете в ЦБ, отклонить перевод, посчитав его подозрительным, автоматически списать сумму, выставленную судебным приставом. И берет комиссию за переводы, например, при оплате услуг ЖКХ.

Бизнес тоже заинтересован в использовании наличности. Бумажные деньги принимаются в любой торговой точке – не нужно покупать терминал, подключать к сети, заключать договор на обслуживание с банком. Не надо ждать, когда деньги клиента придут на счет, что особенно важно в периоды падения курса – деньги, полученные через три дня, могут за это время сильно обесцениться.

Решением может стать цифровой наличный рубль, соединяющий преимущества наличной и безналичной валюты. Рубль, который, подобно обычной купюре, лежит в цифровом кошельке владельца и которым тот может расплачиваться с другим человеком, как бумажной купюрой, без банковских комиссий.

Страсти по криптовалютам

О преимуществах использования цифрового аналога наличных денег говорят уже давно. В 1998 г. компьютерный инженер Вэй Дай изложил идею криптовалюты b-money, а криптограф Ник Сабо – алгоритм децентрализованной цифровой валюты, которую назвал цифровым золотом. В 2009 г. появилась первая практическая реализация идеи – биткоин. К маю 2011 г. стоимость биткоина выросла в 28 раз, успех повлек за собой появление новых криптовалют, таких как Ethereum, Litecoin, Emercoin.

В России отношение к криптовалютам сильно менялось. Сначала они воспринимались как средство расчетов для криминальных элементов. Для этого были основания – взять хотя бы работу сети наркоторговцев Silk Road. За использование криптовалют предлагали ввести уголовную ответственность, причем за особо крупные сделки наказывать строже, чем за убийство.

Историческим стало первое обсуждение криптовалют в Государственной Думе в июне 2016 г., после чего позиция государства смягчилась и начали рассматриваться вопросы легализации цифровых денег. Отмечались важность введения криптовалют в правовое поле, потенциал использования в интернете вещей, польза майнинга для экономики.

Сегодня криптовалюты находятся в «серой» зоне, но общий тренд опять изменился. 31 июля 2020 г. Президент России подписал закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» № 259-ФЗ, запрещающий использовать криптовалюты в качестве средства платежа. Государство пока не запретило криптовалюты безоговорочно с установлением административной и уголовной ответственности, но такое решение уже не удивит.

Что такое «цифровой рубль»?

В криптовалютах власть не устраивает относительная анонимность и невозможность контро-

ля эмиссии – одной из важнейших функций государства. Вместе с тем уже стали понятны преимущества криптовалют для бизнеса, прежде всего в плане снижения транзакционных издержек. Компромиссным вариантом может стать цифровой рубль, материал о котором «Цифровой рубль. Доклад для общественных консультаций» недавно опубликован Банком России.

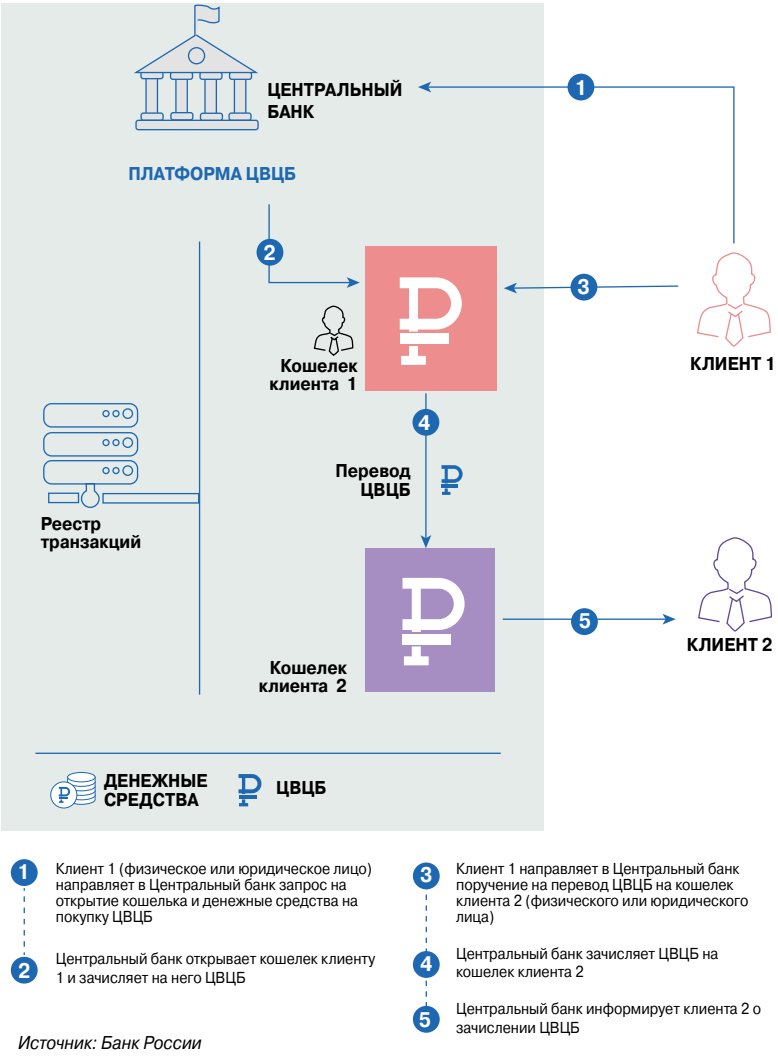
Цифровой рубль – это все тот же российский рубль, который будет выпускаться Банком России в цифровой форме дополнительно к существующим формам денег. Граждане будут иметь возможность зачислять цифровые рубли в свои электронные кошельки и пользоваться ими с помощью мобильных устройств и других носителей, как в онлайн-режиме, так и офлайн, в отсутствие доступа к интернету. В этом случае один из возможных вариантов – расплачиваться цифровыми рублями через интерфейс NFC (Near Field Communication). Не нужно платить банку комиссию за перевод, и, как в случае наличной валюты, деньги продавцу поступают сразу. Они не рвутся, и их труднее украсть.

Цифровой рубль дополнит денежное обращение и будет использоваться одновременно с наличными рублями и средствами населения и предприятий на счетах в банках. Граждане и предприятия смогут свободно переводить свои деньги из одной формы в другую, т.е. из цифрового рубля в наличные или на счет в банке и обратно.

Особо подчеркивается, что цифровой рубль не криптовалюта, т.е. эмитировать его может только Банк России. Наличный рубль имеет серию и номер, цифровой рубль будет иметь уникальный цифровой код. Цифровой рубль будет храниться в индивидуальных электронных кошельках, открытых непосредственно в платежной системе Банка России и являющихся его обязательствами. По сути – каждый сам себе станет банком со своим корсчетом в ЦБ.

Банк России сформулировал требования к цифровому рублю:

- простота использования, поддержка типовых платежных сценариев, например, перевод получателю по номеру его мобильного телефона;
- высокая скорость выполнения операций: платеж цифровым рублем в торгово-сервисных предприятиях не должен занимать больше времени, чем оплата платежными картами или через сервисы мгновенных платежей;
- надежность, успешное выполнение всех операций с вероятностью сбоя, близкой к нулю;
- издержки плательщика при совершении операций с цифровым рублем должны быть не выше, чем при использовании платежных карт и других инструментов розничных платежей;
- повсеместность приема, как у наличных денег;
- безопасность хранения средств в электронном кошельке, уверенность потребителя в низком риске потери средств вследствие взлома или мошенничества;
- удобство и легкость конверсии в наличные и средства на счетах в банках.



Источник: Банк России

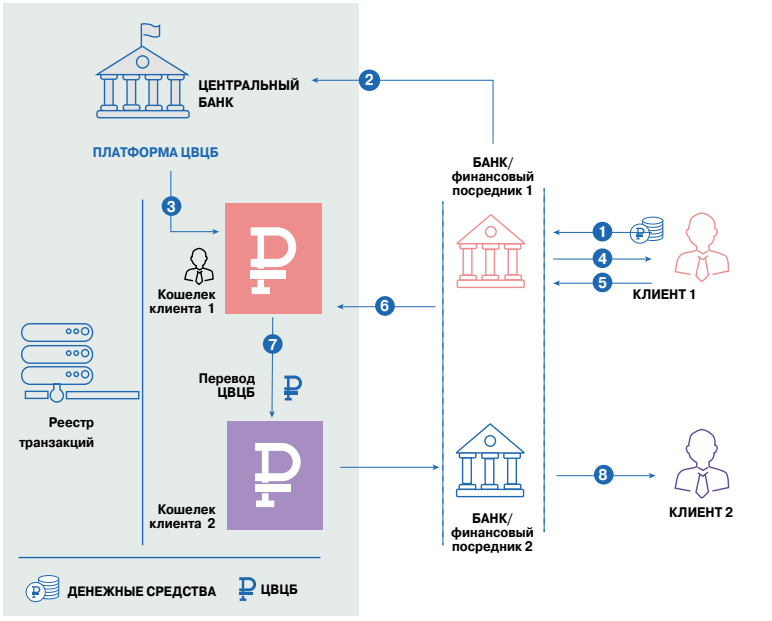
▲ Рис. 1. Взаимодействие обладателей цифровых рублей и ЦБ. Модель B

Также требуется обеспечить бесшовность переводов цифрового рубля с электронного кошелька онлайн на электронный кошелек офлайн и обратно.

Для конверсии средств со счетов в коммерческих банках в цифровой рубль могут быть установлены такие же ограничения, какие существуют для наличных денег, например, необходимость заблаговременно предупреждать банк о снятии крупной суммы со счета.

Модели использования цифрового рубля

Банк России предложил несколько возможных механизмов взаимодействия обладателей цифровых рублей и ЦБ. Наиболее простой и логичный (в опубликованном документе – модель B, рис. 1) предусматривает прямое обраще-



1. Клиент 1 (физическое или юридическое лицо) направляет в банк 1 запрос на открытие кошелька и поручение на покупку ЦВЦБ
2. Банк 1 инициирует открытие кошелька клиента 1 на платформе ЦВЦБ и переводит в Центральный банк денежные средства
3. Центральный банк открывает кошелек клиенту 1, зачисляет на него ЦВЦБ и информирует об этом банк 1
4. Банк 1 информирует клиента 1 об открытии его кошелька и пополнении последнего ЦВЦБ
5. Клиент 1 направляет в банк 1 поручение на перевод ЦВЦБ со своего кошелька на кошелек клиента 2 (физического или юридического лица)
6. Банк 1 инициирует перевод ЦВЦБ с кошелька клиента 1 на кошелек клиента 2
7. Центральный банк проводит списание ЦВЦБ с кошелька клиента 1, зачисляет ее на кошелек клиента 2 и информирует об этом банк 2
8. Банк 2 информирует клиента 2 о зачислении ЦВЦБ на его кошелек

Источник: Банк России

▲ Рис. 2. Взаимодействие обладателей цифровых рублей и ЦБ. Модель С

ние владельца цифрового рубля (клиента) к платформе цифровой валюты Центрального банка (ЦВЦБ). Во всяком случае в этом варианте не надо уплачивать комиссию посредникам.

Финансовым организациям скорее понравится модель С (рис. 2), в которой банки по поручению клиентов инициируют запросы на открытие кошельков и проведение расчетов на платформе ЦВЦБ, а также отправляют запросы на осуществление переводов. Близка к схеме обращения безналичных денег модель D, когда банк-посредник сам открывает кошельки с цифровыми рублями для клиентов и проводит по ним операции.

В качестве механизма технической реализации ЦВЦБ рассматриваются три варианта: распределенный реестр (блокчейн), централизованный реестр, т.е. одна база, в которую записываются все транзакции, и гибридная модель, включающая распределенный и централизованный реестры.

Вопросы для обсуждения

Банк России вынес на обсуждение более десятка вопросов по экономическим и технологическим аспектам введения цифрового рубля. Главный вопрос – нужен ли он вообще?

«В отличие от безналичных рублей, по сути являющихся долговыми расписками банков, цифровой рубль – деньги, которые эмитируются государством. При оплате банковской картой взимаются комиссии в пользу платежных систем, банка – держателя ваших денег. При использовании цифрового рубля посредников нет. Это отличное решение, эффективное с точки зрения экономики, и хорошо, что оно приходит в нашу жизнь. Чем быстрее придет, тем лучше будет людям и обществу», – отметил интернет-омбудсмен Дмитрий Мариничев.

Вопросы вызывает механизм реализации и сама трактовка понятия «цифровой рубль». «Блокчейн решает проблему доверия к оператору платежей. В случае с ЦБ никакого недоверия к оператору нет. Проще создать электронную систему платежей типа “Яндекс.Деньги”, но от лица Банка России, и назвать ее “электронный рубль”, не путая с понятием “цифровой рубль”. При этом не нужно делать блокчейн, и накладные расходы будут в разы меньше», – считает основатель блокчейн-платформы Erachain Дмитрий Ермолаев.

Электронные деньги хорошо себя зарекомендовали, но в России до сих пор не являются полноценным средством платежа. Ограничения заданы законом «О национальной платежной системе» от 27.06.2011 № 161-ФЗ, в котором четко сказано, что электронные деньги запрещено использовать для переводов от юридических лиц. То есть ими не могут расплачиваться все субъекты экономики. На момент принятия закона такое ограничение было оправдано ввиду слабого контроля со стороны Банка России за транзакциями внутри электронных платежных систем. Однако электронная платежная система, запущенная самим ЦБ, будет под полным его контролем, дополнительные ограничения не нужны, и можно сделать полноценный электронный рубль. Электронные деньги – следующий шаг в развитии денег. Такие деньги более технологичны и удобны, чем безналичные банковские платежи. По мнению Дмитрия Ермолаева, перепрыгивать сейчас через эту ступеньку развития денег сразу на «цифровые деньги» еще рано.

Эксперт также выразил сомнение в возможности реализации оплаты в режиме офлайн: «Даже при использовании блокчейна с множеством защищающих его нод транзакция вне сети может породить двусмысленность. Например, при платежах рублями с одними и теми же цифровыми кодами за разные товары. Если нет доступа к децентрализованной базе блокчейна, то проверить на лету, кому переведены цифровые рубли, невозможно».

В целом инициатива Банка России – шаг в правильном направлении. Идея снижения издержек за счет уменьшения стоимости транзакций и числа посредников выглядит привлекательной. Вопрос в конкретной реализации, учитывающей интересы населения и игроков рынка. ИКС

Трансформация 2020: условие для эволюции ИТ-бизнеса

Для выживания в стремительно меняющемся мире бизнес должен шире использовать цифровые технологии. О том, как Rittal помогает компаниям оперативно разворачивать или модернизировать ИТ-инфраструктуру, – Кирилл Дмитриев, главный технический специалист по ИТ-проектам Rittal.

– Кирилл, как текущая мировая ситуация влияет на развитие ИТ-сферы? Какие решения приоритетны для рынка и где они применяются?

– В современных условиях компании самых разных направлений бизнеса все чаще переходят на электронный формат взаимодействия с клиентами. В качестве примера возьмем рынок электронной коммерции США, который, по данным отчета коммерческого отдела Bank of America, удвоился за первую половину 2020 г. Если в 2019 г. доля электронной торговли в розничной составляла 16%, то в апреле 2020-го – уже 27%.

Вторым после торговли приоритетным направлением для рынка ИТ является промышленность: нефтехимия, газовая отрасль, горнодобывающая промышленность. Бизнес стал лучше понимать преимущества использования цифровых технологий для мониторинга производственных процессов и управления ими. Развиваются технологии Индустрии 4.0, причем на производстве вычислительные системы зачастую работают в неблагоприятных условиях повышенных температур, влажности и запыленности, что требует применения специфических технических решений для поддержания их функционирования.

Третье направление – интернет вещей, например, инфраструктура для транспорта. С огромной скоростью строятся станции метро, дорожные развязки, транспортные пересадочные узлы. Для анализа ситуации на дорогах и управления транспортными потоками нужны решения, размещаемые на улицах, защищенные от осадков и вандализма, обеспечивающие необходимые параметры микроклимата для работы вычислительных систем, собирающие информацию о пробках, оплате парковок, нарушениях ПДД. Если раньше квитанции о штрафах шли неделями, то сейчас «письма счастья» приходят на следующий день после нарушения. Контент должен обрабатываться с учетом данных геолокации, максимально быстро и качественно, чтобы снизить риск ложных срабатываний и возникновения недовольства у владельцев транспортных средств.

Приоритетными становятся решения для предприятий малого и среднего бизнеса, активно переходящих на цифровые модели работы. Растет спрос на компактные решения, которые можно быстро и с минимальными затратами разместить в непосредственной близости от места сбора данных и которые способны обеспечить высокий уровень надежности работы вычислительных систем.

– Как вендорам адаптироваться к новым условиям? Как повысить внутреннюю компетенцию, чтобы понимать, что нужно заказчику?

– Для решения новых задач недостаточно просто продавать коробки с компонентами. Чтобы находиться в тренде, надо предлагать законченные решения по принципу plug & play – «включил и работает». Если заказчик имеет только концепцию проекта, то задача вендора не просто предложить выбрать что-либо из каталога, а рекомендовать максимально сбалансированное решение, которое удовлетворяет требованиям конкретной задачи и учитывает специфику проекта. Ведь все проекты по сути – уникальные.

Чтобы понимать заказчика, выступать в роли не только поставщика, но и системного консультанта, компания должна иметь опыт и компетентных специалистов. Для предоставления заказчику сбалансированного решения компания должна обладать экспертизой в реализации самых разных проектов.

Только решив множество конкретных практических задач при внедрении проектов, компания может утверждать, что имеет опыт в этой сфере. У Rittal накоплен опыт при создании разнообразных дата-центров – от микроЦОДов размером в одну стойку до крупных ЦОДов, построенных по модульной технологии. В своих проектах мы используем экспертизу, полученную не только в России. Например, в компании регулярно проводятся международные конференции для обмена опытом между представительствами, где представляются и анализируются лучшие, самые неординарные и технически сложные проекты.

Еще одним важным фактором является честность и открытость по отношению к партнеру. Прозрачность взаимоотношений – ключ к длительному плодотворному сотрудничеству.

– Удачное ли сейчас время для запуска новых линеек оборудования, расширения портфолио, модерни-

зации продуктов? Может ли текущая ситуация стать толчком для появления пионеров в ИТ-сфере?

– В этом году Rittal сделала новый шаг в ИТ-направлении, ставший переломным моментом в ее истории. Компания выпустила на рынок новую платформу продуктов RiMatrix NG, которая полностью обновляет портфолио для ИТ-инфраструктуры. Новые стойки, PDU, источники бесперебойного питания, обновление систем мониторинга и охлаждения. Компания готова применять обновленные решения и использовать их преимущества в новых проектах.

Раньше ИТ-рынок был замкнутым, на него было трудно войти и потеснить корифеев. Сейчас благодаря бурным процессам цифровой трансформации появляется много пионеров-первопроходцев. Компании самых разных отраслей переходят на цифровые рельсы, причем в срочном порядке. Одни выберут облака, другие – корпоративные дата-центры. Будут строиться большие и маленькие ЦОДы. Многие, прежде всего конечные заказчики, не сразу будут понимать – что и как они хотят реализовать. Важно помочь им выбрать правильное и гибкое решение. Предлагаемое оборудование должно обладать модульностью, масштабируемостью и совместимостью с существующей инженерной инфраструктурой.

– Как период спада влияет на конкуренцию? Как найти в бывшем конкуренте надежного партнера и взаимно усилиться?

– Период нестабильности – хорошее время для объединений. Лучший пример – коллаборация компаний Stulz и Rittal, партнерство которых началось в этом году. Причем мы сотрудничаем не только на уровне штаб-квартир в Германии, но и на уровне локальных представительств, в том числе в России, где Rittal взаимодействует с Hosser Telecom Solutions – крупнейшим дистрибьютором прецизионных систем кондиционирования Stulz на территории нашей страны. Stulz имеет заслуженно высокую репутацию на рынке прецизионного охлаждения, а Rittal – в ИТ-шкафах, PDU, ИБП, мониторинге. Объединение компетенций, синергия продуктов расширяют круг задач, которые могут решать компании.

– Какие услуги нужны партнеру? Как повысить вовлеченность и заинтересованность заказчика в конечном результате?

– Не все заказчики хотят детально разбираться в технической документации, ориентироваться в проектных планах, не все воспринимают 2D-формат чертежей. Из спецификации не до конца понятно, что получит заказчик. Для максимального упрощения взаимодействия поставщика, интегратора и заказчика надо не просто давать файл в формате Excel с табличкой спецификации, а предоставлять исчерпывающую информацию о решении в целом. Rittal делает описание всех подсистем, поясняет, как они интегрируются, почему выбрано именно это оборудование, а не другое, чтобы заказчик понял, что ему предлагается не самое дорогое решение, а наиболее отвечающее техническому заданию.

Когда техническое решение выбрано и началось проектирование, необходимо понимание объемно-планировочных решений и компоновки оборудования. Надо готовить чертежи и 3D-визуализацию. Rittal оказывает поддержку и на этом этапе, предоставляет визуальные и графические материалы для проектировщиков и интеграторов из своей обширной электронной библиотеки. Благодаря этому заказчик сможет увидеть, как будет выглядеть объект в результате выполнения работ.

Важный этап – математическое моделирование микроклимата будущего ЦОДа, базирующееся на проектном решении и предоставляемой заказчиком информации об удельной тепловой нагрузке на стойку. Потребитель сможет увидеть, как будет работать еще не построенный ЦОД: будет ли достаточной циркуляция воздуха, не возникнут ли локальные зоны перегрева, что произойдет в аварийной ситуации при выходе оборудования из строя. Результат моделирования – трехмерные модели температур, скоростей перемещения воздуха, указание потенциально проблемных зон. Это немаловажный фактор, позволяющий оценить техническую грамотность и надежность предлагаемой инженерной инфраструктуры.

– Какие задачи ставит перед собой Rittal в 2020–2021 гг.?

– Ситуация в мире стремительно меняется. Появляется много новых заказчиков с разными, зачастую уникальными запросами. С учетом этого необходимо разработать как можно больше готовых решений, чтобы заказчики получали и разворачивали инфраструктуру с максимальной скоростью. Rittal хочет участвовать не только в долгосрочных проектах, но и в оперативном предоставлении инфраструктуры. Не зря свой новый шкаф Rittal VX IT мы характеризуем как самый быстрый ИТ-шкаф в мире. Предложить готовые решения с короткими сроками поставки, чтобы любой клиент вне зависимости от запросов разворачивал инфраструктуру тогда, когда ему нужно, – вот настоящий вызов будущего.

Мы стремимся наращивать компетенцию, делиться опытом с партнерами и заказчиками, повышать уровень вовлеченности в проектную деятельность, участвовать в проекте с начала предварительных обсуждений и до его полного завершения. Выбор решения и интеграция с существующими системами должны быть продуманы с самого начала. Только при таком подходе можно гарантировать высокую эффективность и точность примененного решения.

Документы в «бронированных» облаках

Роман Трейнис, технический директор, «Тионикс»

Почему цифровизация документооборота и перенос баз данных в облака – процесс неизбежный, но в случае государственных систем такой долгий, и почему важно помнить об этом сейчас?

Когда в начале весны люди по всей стране по объективным причинам оказались массово удалены от рабочих мест и порой были лишены возможности выполнять свои служебные обязанности либо были вынуждены выполнять их с риском для себя и работодателя, вопрос об организации удаленных рабочих мест и ведении документооборота в электронной форме встал остро. Особенно это было заметно в госучреждениях. Государство не может перестать работать ни при каких условиях, поскольку если оно не работает – его нет.

По данным на конец 2019 г., в России насчитывалось порядка 855 тыс. государственных гражданских служащих. Из них 603 тыс. человек – федеральные гражданские служащие, 252 тыс. – гражданские служащие регионов. В органах местного самоуправления работают еще 395 тыс. муниципальных служащих. Если считать не только служащих, а всех работников государственных и муниципальных органов, получится 2,4 млн человек, что составляет 3,3% общей численности занятых в экономике. В то же время, по данным Правительства Москвы, только в столице 2,9 млн пользователей электронного документооборота ежедневно создают около 50 тыс. документов и 75 тыс. резолюций. Это большой и сложный механизм, работу которого невозможно остановить, который должен работать точно, особенно в тяжелые времена, когда решения необходимо принимать быстро и четко. А еще в такие периоды важно максимально сократить издержки и оптимизировать возможные затраты.

Все это достаточно очевидно. Кроме того, в России уже с 2011 г. реализуется проект формирования электронного правительства, но здесь есть свои сложности.

Электронный – не облачный

Сегодня, с одной стороны, сама жизнь подталкивает госучреждения двигаться в русле технологического прогресса, цифровизации и открытости, а с другой – над ними довлеет необходимость соблюдать самую высокую степень закрытости, осторожности и безопасности.

В России облачная модель признана основной архитектурой для электронного правительства. Разработаны правовая база и нормативные технические требования. Уже действуют такие информационные системы, как Единый портал госуслуг, Система электронного межведомственного взаимодействия (СМЭВ), Единая система идентификации и аутентификации, единое пространство доверия электронной подписи, единая система справочников и классификаторов (используемых в государственных информационных системах, ГИС), система координации, обеспечивающая формирование единого информационного пространства в сфере управления ИКТ в госсекторе, национальная платформа предоставления сервисов удаленной обработки и хранения данных.

Тем не менее доля госучреждений и предприятий госсектора, перешедших на облачные технологии, самим правительством оценивается менее чем в 50%. И дело не только в том, что госсектору в широком смысле свойственны косность и неторопливость (а именно таково обывательское представление о бюрократических структурах). Существуют объективные и субъективные факторы, связанные с сохранностью данных и тормозящие переход к облачным решениям. По оценке аналитического центра компании InfoWatch, всего за год, с 2017-го по 2018-й, число масштабных утечек информации из облачных хранилищ возросло на 43%. На фоне такой статистики необходимо понять, насколько безопасно и действительно нужно переносить системы в облака, какие из факторов, влияющих на процесс, субъективны, а какие нет.

Что надо ГИС

Скорость бумажного документооборота невелика. Найти что-либо в нецифровых архивах

информации крайне сложно. Хранение огромных архивов данных – процесс затратный. Получить доступ к нужной информации или документам, не находясь физически в расположении архива, невозможно. Поэтому интерес к облачным технологиям понятен.

Особый интерес для органов государственной власти представляют:

- межведомственное взаимодействие и работа с обращениями;
- государственные услуги в электронном виде;
- решение ведомственных задач.

Свои желания государственная система формулировать умеет. Еще с 2006 г. действует Федеральный закон ФЗ-149 «Об информации, информационных технологиях и о защите информации». Во исполнение требований данного закона был издан Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». В 2017 г. были приняты дополнения к этому приказу, касающиеся мер безопасности. Всего существуют четыре класса безопасности, из который первый – самый высокий. ГОСТ 34.601 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» регламентирует качество систем. Таким образом, регламентирующих документов достаточно. В чем же проблема? Проблема – в психологии и статистике, оказывающей на нее непосредственное влияние.

Проблема в головах

Чтобы понять, каким образом статистика влияет на принятие решений в области ГИС, вернемся к цифрам отчета InfoWatch. Количество утечек действительно всего за год выросло более чем на 40%, однако важно понимать, что это общая цифра. Большая часть утечек произошла в частном секторе. В указанный период более 25% всех утечек пришлись на облачное хранилище компании Amazon. Таким образом, если вывести за рамки подсчета нерелевантные примеры, статистика перестанет быть столь пугающей.

Это вовсе не означает, что угрозы взлома или утечки данных по неосторожности не существует. Количество киберугроз увеличивается вместе с ростом уровня цифровизации, но одновременно развивается инструментарий борьбы с ними, а также накапливается опыт у людей, занимающихся защитой данных.

Провайдеры облачных услуг обладают большим набором инструментов, которые позволяют им гарантировать клиентам безопасность данных. Для организации защищенных каналов связи в ЦОДе сервис-провайдеры используют отказоустойчивые кластеры координаторов, например маршрутизаторов. Для увеличения пропускной способности каналов связи и в качестве дополнительного механизма резервирования производится настройка агрегации каналов связи. Организуются защищенные системы передачи данных (ЗСПД) с использованием сложной криптографии. Осуществляется контроль обмена трафиком между криптошлюзами СМЭВ, каналами ЦОДа и ЗСПД.

Заказчик должен найти проверенного и качественного провайдера. Потенциальный поставщик облачных услуг должен выполнять все требования по обеспечению защиты информации, предъявляемые к государственным информационным системам и информационным системам персональных данных, обладать распределенной сетью дата-центров и собственными волоконно-оптическими сетями.

Если соблюдать все эти требования, риск можно свести к минимуму.

Проблема в головах-2

Другая важная проблема при переходе на облачные технологии – непонимание своих потребностей, неумение пользоваться сторонними сервисами, вести работу с подрядчиком цифровых услуг. Одна из целей миграции в облако – экономия. Согласно данным госкомпаний, когда каждая организация строит собственную цифровую инфраструктуру, ее оборудование задействуется в лучшем случае на 30% мощности. Переход же на IaaS-сервисы у облачного провайдера позволяет повысить уровень эффективности потребления вычислительных мощностей до 70–95%. Однако, как показывает практика, многие компании, обратившись к облачным сервисам подрядчика, экономят за счет сокращения штата своих ИТ-специалистов, а не благодаря рациональному использованию нового сервиса.

Как свидетельствует опрос более 3 тыс. компаний из почти 30 стран мира, проведенный исследовательской компанией ReRez совместно с Symantec, большинство организаций рационально используют облачные мощности только на 17%. Больше половины опрошенных признались, что практически не уделяют внимания таким аспектам, как удаление дублированных данных или использование мощностей. Компании арендуют в два раза больше ресурсов, чем им на самом деле нужно.

Подрядный сервис – это средство сэкономить, но в головах людей продолжают работать старые схемы, по которым счета за облачные услуги приходят раз в месяц, как за услуги ЖКХ, и лезть в «магию» их формирования бес-

смысленно. А еще срабатывает принцип – «не волнует, уплачено». В таких условиях легко расслабиться и перестать следить за потреблением ресурсов. Это тоже момент психологический, арендуемые мощности не воспринимаются как свои, отсюда невнимательность и нерациональное расходование средств.

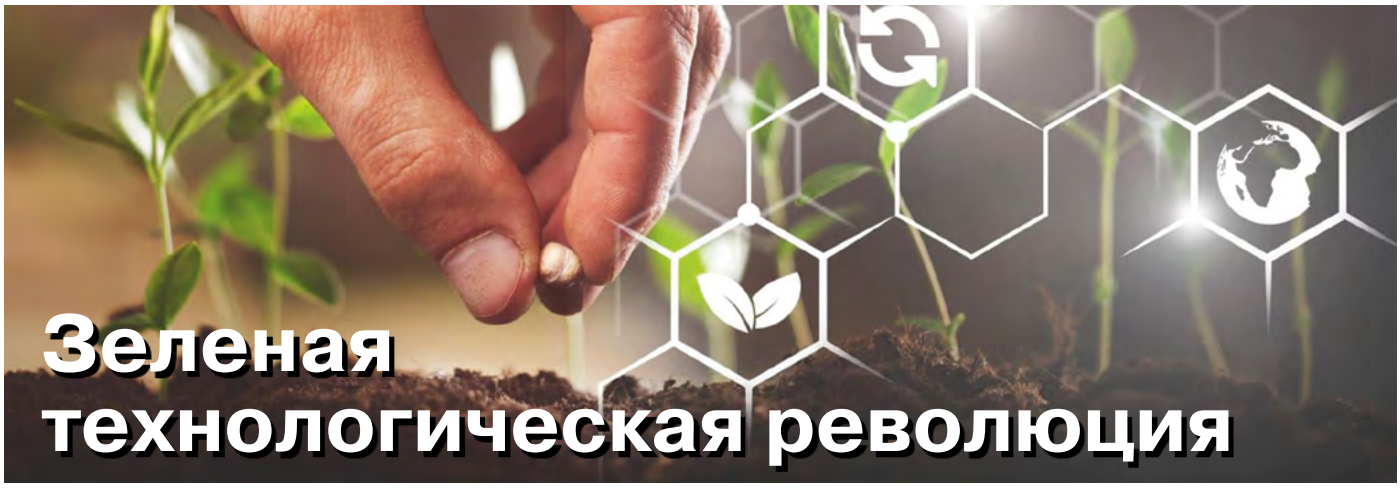
Ценность облачного сервиса заключается в том, что оплачивать можно лишь конкретно потребляемые ресурсы. Для начала, например, можно удалить и отключить виртуальные машины, которыми вообще не пользуются, или настроить работу с ними в выделенный период времени. Более долгий способ – воспитание культуры работы с виртуальными мощностями: следить за излишним дублированием информации, не хранить информацию, которая не нужна, и вести такую работу регулярно. Подобные привычки, как раздельный сбор мусора, вырабатываются постепенно.

Те компании, которые смогли грамотно организовать работу с облачными сервисами, сообщают о том, что снижение расходов на ИТ у них составило не 30–40, а 50%.

Каковы перспективы

Основные драйверы роста спроса на облачные технологии со стороны государства – повышение эффективности предоставления услуг и сокращение госрасходов. В 2019 г. аналитики P&S прогнозировали рост рынка облачных услуг для госсектора на уровне более 10% в год до 2022 г. Среди самых перспективных направлений выделяли системы хранения и аварийного восстановления данных, управление идентификацией и доступом к информационным ресурсам (IAM), управление рисками (RCM). Однако эти прогнозы были сделаны до пандемии коронавируса, когда всем пришлось внезапно осознать облачные технологии не только как моду, но как насущную потребность. Посткоронавирусный период сделает вопрос еще более актуальным, и не только с точки зрения технологий, но и с точки зрения экономии бюджетных средств.

Однако важно, чтобы заказчик в лице любого государственного ведомства понимал цели и задачи, для которых технологии осваиваются, и мог пользоваться такими услугами рационально. ИКС



Зеленая технологическая революция

Цифровизация стала частью повседневной жизни. Даже одна из самых консервативных отраслей – агропромышленный комплекс – осваивает современные технологические разработки.

Виолетта Аралова, корреспондент, «Цифровой океан»

Эксперты сходятся во мнении: будущее сельского хозяйства во всем мире зависит от того, насколько АПК готов воспользоваться преимуществами цифровой трансформации. По прогнозам ООН, население мира к 2050 г. достигнет 9,8 млрд человек. Чтобы его прокормить, нужно увеличить производство продовольствия на 70%. Сельское хозяйство по всему миру должно изменить процессы производства, сделать их продуктивными и эффективными.

Крупные холдинги готовы инвестировать в новые технологии, вкладывать средства в цифровые системы и способствовать их повсеместному распространению. По мнению экспертов, именно те компании, которые в ближайшем будущем объединят бизнес в единую систему на основе цифровой платформы, и станут безусловными лидерами рынка.

Внедрение цифровых решений в АПК не просто очередная кампания по повышению продуктивности, это вызов отрасли, настоящая «зеленая революция».

Федеральный проект «Цифровое сельское хозяйство»

К решению проблемы в России подключились федеральные власти. Частью национального проекта «Цифровая экономика РФ» стал федеральный проект «Цифровое сельское хозяйство». Его цель – модернизация аграрной отрасли и повышение производительности на «цифровых» сельскохозяйственных предприятиях в два раза к 2024 г. В планах – оцифровка земель, подготовка новых кадров и запуск единой национальной цифровой платформы.

О внедрении информационных технологий в АПК говорится и в «дорожных картах» FoodNet и AeroNet Национальной технологической инициативы. Сфера их интересов – создание концепции «умного» сельского хозяйства с помощью грантов и возвратных инвестиций в сумме 3,3 млрд руб.

В Минсельхозе России прогнозируют, что общий прирост продукции сельского хозяйства в результате цифровизации может составить 361,4 млрд руб., а ожидаемый прирост продукции растениеводства – 193,9 млрд руб., или 7,5% объема произведенной продукции в фактических ценах по итогам 2018 г. Уровень цифровизации сельского хозяйства может вырасти в ближайшие 10 лет в три-четыре раза в индексном выражении.

Представители отрасли уверены, что через 10 лет более 80% российских сельхозпроизводителей будут применять цифровые решения.

Какие технологии используются в сельском хозяйстве сегодня?

«Фермерам и агропредприятиям нужно справляться с проблемами плохих всходов, выявлять очаги болезней, научиться с высокой точностью прогнозировать урожаи, чтобы планировать другие работы производственного цикла: сбор, транспортировку, хранение, реализацию продукции, – говорит соучредитель и главный исполнительный директор компании iFarm Максим Чижов. – Здесь эффективны технологии компьютерного зрения, машинного обучения, а также автоматизация и роботизация многих процессов, включая посадку и сбор урожая».

Уже сейчас востребованы технологии спутникового позиционирования, ГИС-системы и системы мониторинга и контроля техники и качества выполнения работ. Развивается рынок систем управления предприятием (ERP), систем контроля и учета в различных отраслях агропроизводства, специализированных данных и ПО для принятия своевременных решений.


Ifarmproject.ru

Набирают популярность дроны – с их помощью фермеры осуществляют мониторинг состояния полей, проводят аэрофотосъемку, орошают земли и даже засевают территории.

Например, анализ снимков NDVI (карта показателей количества фотосинтетически активной биомассы) десятков тысяч гектаров пашни, подсчет количества плодов на тысячах гектаров садов позволяют своевременно и точечно решать проблемы плохих всходов, недостаточной зеленой массы, выявлять очаги распространения болезней и вредителей, прогнозировать урожай и планировать уборочные, транспортные, складские мощности и/или работы.

Нейросети следят за здоровьем растений

В марте нынешнего года Россельхозбанк сообщил, что включит сервис диагностики здоровья растений в собственную цифровую экосистему. Нейросеть, которая может обнаружить фитопатологию по фотографии, банк разрабатывает совместно с Институтом проблем управления им. В.А. Трапезникова Российской академии наук.

Директор Центра развития финансовых технологий Россельхозбанка Елена Батурова отметила: «Прикладная задача создания нейросети, которая по фотоснимку определяет наличие или отсутствие заболевания у яблони, без труда может быть масштабирована для других видов деревьев и растений. Это яркий пример того, как современные цифровые технологии будут помогать фермерам и агропредприятиям в их работе».

По мнению руководителя дивизиона «Сады» агрохолдинга «АФГ Националь» Олега Рьянова, развитие цифровых технологий и автоматизация процессов диагностики позволяет уменьшить влияние человеческого фактора и вероятность ошибки, способствует сокращению нагрузки на персонал и росту эффективности труда.


Фото: prokazan.ru

Интернет вещей в сельском хозяйстве

В апреле 2020 г. «Деревенский молочный завод» сообщил о начале использования разработанной МТС IoT-системы контроля за поголовьем скота в животноводческих хозяйствах. Представитель МТС Алексей Меркутов рассказал, что за температурой коров, количеством выпитой ими воды и двигательной активностью следят специальные радиодатчики, которые животные проглатывают вместе с кормом.

Датчики весят около 300 г, они оседают на дне желудка коровы и остаются там на протяжении всей жизни животного. Информация, которую они регистрируют, попадает в аналитическую систему.

Подключение стоит до 500 руб. в месяц на одно животное. Но есть и другие варианты датчиков для коров, например, от компаний Huawei и SAP – одни устройства животные проглатывают, другие фермеры вешают им на шею.

Агролаборатории и вертикальные теплицы

В 2016-м компания Panasonic начала сотрудничество с фондом «Сколково», и через год в здании технопарка была оборудована агролаборатория, где на площади 75 кв. м разместилась пилотная вертикальная теплица. В 2019 г. компания «РусЭко» запустила в Москве городскую ферму для выращивания зелени и ягод.

Компания iFarm разрабатывает и выводит на международный рынок технологии круглогодичного выращивания овощей, ягод и зелени: быстровозводимые автоматизированные вертикальные фермы и ИТ-платформу iFarm Growtune для управления ими. Клиенты компании могут строить собственные фермы и выращивать большой ассортимент культур, не обладая при этом агрономическими знаниями, – созданные в лабораториях iFarm технологические карты для более 120 видов съедобных растений содержат всю необходимую информацию. Вертикальные фермы по технологиям iFarm работают или находятся на стадии проектирования в Европе, России и Казахстане. Как отмечает М. Чижов, технологии iFarm в сравнении с традиционным земледелием исключают риски, связанные с внешними сезонными факторами; не требуют сложных логистических цепочек поставок готовой продукции, экономят время на доставку и исключают потери при транспортировке; экономят природные ресурсы, требуя на производство урожаев до 90% меньше воды и до 99% меньше площади земли; исключают использование химикатов и пестицидов для борьбы с вредителями.

В России есть и технологии «умного» орошения: в Подмосковье компания «Белая дача Фарминг» регулирует нормы полива по специальной цифровой карте, которая анализирует влажность отдельных участков пашни.

Роботы-фермеры

Роботы уже используются для прополки сорняков, для посева и сборки урожая, выполняют точное опрыскивание.

Искусственный интеллект позволяет внедрять полностью автоматизированные производства. Так, самый крупный производитель и поставщик яиц в Татарстане Yaratelle автоматизировал процессы сбора и движения яиц – ими управляет искусственный интеллект на базе программного продукта Amaks. Яйца движутся по транспортеру длиной более 1,5 км, автоматическая сортировальная машина Моба их взвешивает, отбраковывает и упаковывает.

Группа «Черкизово» открыла в Московской области первый в России роботизированный завод по производству сырокопченых колбас «Черкизово-Кашира», который не имеет аналогов в Европе. «Процесс производства полностью автоматизирован – от склада сырья до упаковки готовой продукции. Система технического обслуживания также интегрирована в ERP завода и управляет автоматическим заказом запчастей, – рассказал генеральный директор Черкизовского мясоперерабатывающего завода Сергей Михайлов. – Автоматизация практически исключает негативное влияние человеческого фактора на производственные процессы».

Как ускорить цифровизацию отрасли АПК

Цифровизация АПК в России пока идет медленно. Центр прогнозирования и мониторинга НТР АПК КубГАУ провел исследование и выяснил следующее:

- 33% руководителей хозяйств в России сдержанно относятся к современным технологиям из-за их высокой стоимости, еще столько же не имеют достаточной информации о преимуществах цифровизации;
- 15% сомневаются в функциональности технологий и надежности современной техники;
- 9% считают, что внедрение новых технологий повлечет за собой расходы на переквалификацию персонала.

Как отмечает Николай Бобров, генеральный директор компании «Диджитал Агро», российского поставщика ИТ-решений для АПК, чтобы цифровизация сектора набрала темп, необходимо прежде всего решить вопрос с доступом в интернет. «Крупные телеком-компании должны вместе с государством обеспечить покрытие, в том числе для передачи данных. Мы до сих пор часто попадаем в ситуации, когда доступа в интернет нет даже на трассе, не говоря уже о полях. О какой цифровизации можно говорить в таких условиях? Необходимо построить эту инфраструктуру», – подчеркивает он.

Вторая задача – субсидирование покупки программного и аппаратного обеспечения. «Это основной барьер для входа. Допустим, мы можем продать лицензию на наше ПО дешевле. Но ведь одного ПО мало – нужны датчики, которые устанавливаются на технику и в полях. А они стоят серьезных денег. По нашим подсчетам, на субсидирование приобретения ПО хватит суммы порядка 16 млрд руб. – не такие большие деньги в масштабах страны», – считает Н. Бобров.

Еще одна проблема – нехватка квалифицированных специалистов. Фермеры старшего поколения не очень охотно погружаются в тему цифровизации.

«Главные изменения будут связаны в первую очередь с технологиями, – указывает Алексей Петунин, заместитель генерального директора SAP CIS. – Уже сейчас в России есть пилоты по внедрению машинного обучения. Через пять лет эти технологии войдут в повседневное использование. Одним из основных трендов станет бизнес-платформа со встроенными экспертными системами, которая позволит интегрировать в рамках бизнес-сети поставщиков технологий и технологического контента, сельхозпроизводителей и производителей потребительских товаров».

По мнению Дениса Запасникова, руководителя дивизиона «Поволжье – Юг» компании «Мустанг технологии кормления», кардинальных изменений в секторе молочного животноводства не предвидится, они носят эволюционный характер. «В связи с широким использованием автоматизированных программ учета и управления на молочно-товарных фермах и комплексах уже сейчас есть спрос на специалистов, которые могут анализировать данные, делать прогнозы и предлагать оптимальные решения», – говорит Д. Запасников.

М. Чижов из iFarm считает, что в сельском хозяйстве распространяется тенденция к локализации производства: «Экосистемы, направленные на локальное выращивание в городах и в непосредственной близости от места потребления, выходят на первый план во всем мире. Это обусловлено вопросами продовольственной безопасности. С одной стороны, такие технологии дают возможность выращивать натуральные овощи, ягоды и зелень без пестицидов и обработки химикатами. С другой стороны, локализация производства стала актуальной из-за пандемии, когда мир столкнулся с закрытием границ, что оказало влияние на сроки поставок и прибытие трудовых мигрантов на посевные и уборочные работы». Кроме того, по мнению М. Чижова, аграрный сектор нуждается в большом количестве точной информации – а значит, наибольшей популярностью будут пользоваться различные системы мониторинга, которые позволят заблаговременно определять проблемные участки и принимать решения, направленные на их устранение. Также, замечает эксперт, будут важны системы планирования и управления логистикой, с помощью которых фермеры могут определять необходимый объем посадок под отгрузки, ориентируясь на заказы и складские остатки и избегая таким образом перепроизводства.

Исследователи и аграрии сходятся во мнении: будущие системы производства питания неотделимы от инноваций. Поэтому сейчас настало время сделать шаг вперед – и начать революцию в сельском хозяйстве. ИКС


Фото: kachestvo.pro

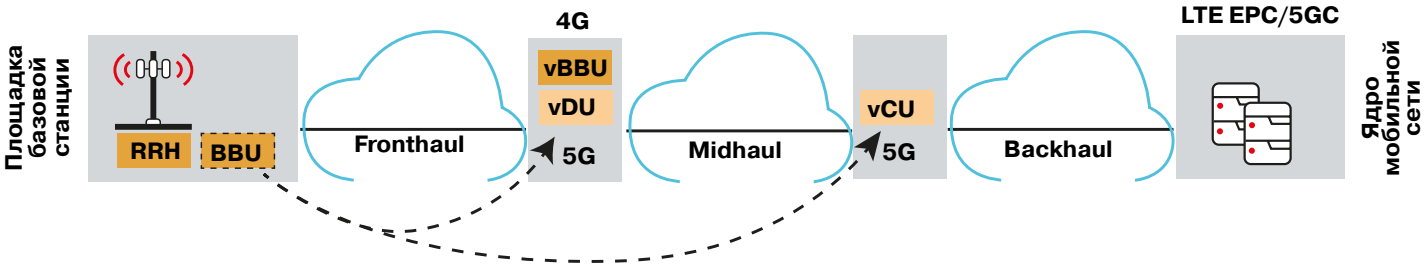
Open RAN – имя нарицательное?

Андрей Абрамов,
менеджер по развитию бизнеса,
НТО «ИРЭ-Полюс»

Концепция Open RAN может стать основой для успешного развертывания 5G в нашей стране при широком использовании отечественного оборудования в сети радиодоступа. Но для этого необходимо обеспечить взаимную совместимость радиомодулей и узлов цифровой обработки базовых станций разных производителей.

В русском языке имена существительные делятся на собственные и нарицательные. Слово «нарицательное» образовалось от старославянского «говорить» и характеризует группу объектов с общими признаками. Например, девочка, торговый центр, кошка. Open RAN тоже можно отнести к этой категории.

Общими признаками объектов «Open RAN» являются новая архитектура базовой станции (рис. 1) с возможностью централизации и виртуализации узлов цифровой обработки (Baseband Unit, BBU), их дезагрегации на функции реального времени (Distributed Unit, DU) и фоновых вычислений (Centralized Unit, CU), открытые интерфейсы, виртуализация, применение больших данных и искусственного интеллекта.



▲ **Рис. 1. Архитектура базовой станции 5G**

В практической области появление концепции Open RAN пока заметно мало. Строительство сетей 5G, как и сетей 4G, идет на оборудовании традиционных производителей (Nokia, Ericsson, Huawei). Этот путь для операторов наиболее экономичен и исключает риски для существующего бизнеса. Коммерческие внедрения оборудования Open RAN единичны, и уровень зрелости таких решений пока не ясен. При этом отсутствие функционального паритета с традиционными поставщиками не дает возможности рассматривать Open RAN на существующей сети мобильного оператора.

Альянс O-RAN, выдвинувший концепцию Open RAN, активно пытается ее конкретизировать. Однако Open RAN до сих пор не воспринимается как законченное решение. Одна из основных причин такого положения – разные интересы участников отраслевой инициативы, трактующих Open RAN с позиций своих бизнес-моделей:

- Для производителей IP/Ethernet-транспорта Open RAN – это прежде всего пакетный интерфейс eCPRI (enhanced Common Public Radio Interface) между радиомодулями (Radio Remote Head, RRH) и BBU/DU. Производители рассчитывают, что такой интерфейс позволит им расширить продажи на новый транспортный домен – Fronthaul.
- Для мобильных операторов Open RAN – это один из инструментов усиления конкуренции с целью снижения цен на рынке, а также необходимое условие минимизации технологических рисков. Актуальность последнего фактора стала очевидной в последнее время, когда выяснилось, что выполнение политических решений о полной замене сетевого оборудования одного поставщика на оборудование другого наталкивается на отсутствие на рынке необходимых ресурсов и компетенций.
- Новым производителям оборудования радиодоступа в Open RAN важна совместимость между их программным обеспечением и аппаратными платформами RRH, BBU, DU, CU, а также централизованная архитектура радиосети с единым пулом вычислительных ресурсов для нескольких базовых станций. Первое позволяет использовать аппаратные платформы на базе открытых спецификаций, а второе – повысить эффективность виртуализации.

Несмотря на то что перечисленные цели друг другу не противоречат, учет интересов каждой стороны снижает эффективность практического внедрения Open RAN и уменьшает размер рыночной ниши.

В России внедрение Open RAN рассматривается также в русле поддержки отечественной промышленности и обеспечения безопасности. Поэтому задача усложняется объективными противоречиями между мобильными операторами, отечественными производителями и государственными структурами:

- Операторы не готовы обсуждать внедрение отечественного оборудования в силу высокого риска потерять конкурентоспособность и возможность предоставлять качественные услуги, за которые абоненты будут платить.
- Отечественные производители не могут достичь функционального паритета в короткий срок до развертывания сетей 5G.
- Государство не готово выдать лицензии и частоты, поскольку не решены вопросы внедрения отечественного оборудования и безопасности.

Проблемы локализации при внедрении Open RAN в той или иной мере стоят и в других странах, и до сих пор нет какого-либо глобального подхода, который можно использовать. Однако, пожалуй, только в России эта, казалось бы, новая коммерческая возможность рассматривается мобильными операторами как дополнительное обременение, размер и форма которого определяются сегодня диктатом со стороны государства.

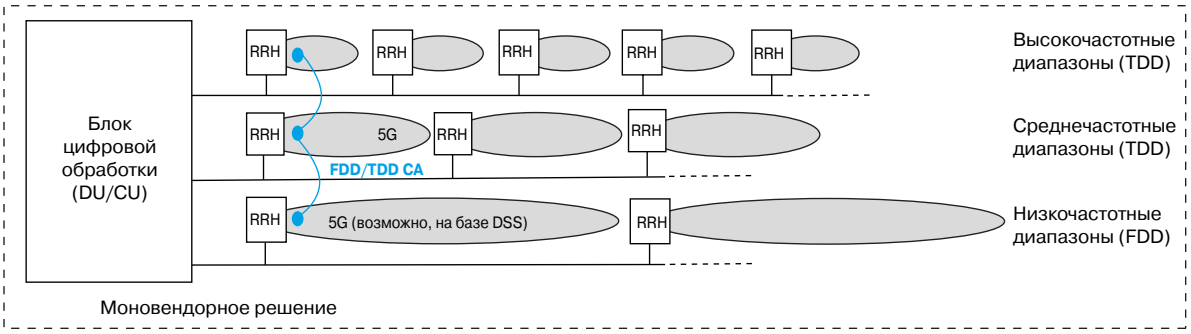


Рис. 2. Целевая архитектура 5G RAN ▶

К настоящему времени в мире накоплен определенный опыт строительства систем 5G, который позволяет вернуться к решению задач внедрения Open RAN на российском рынке и развития отечественной промышленности в более конструктивном ключе. В основе предлагаемого анализа лежит оценка возможности построения целевой архитектуры 5G RAN на мультивендорном оборудовании без рисков ограничения потребительских качеств.

Целевая архитектура 5G RAN

Частотные ресурсы, за счет которых достигаются высокие скорости 5G, лежат в более высоких, чем для LTE, частотных диапазонах. А поскольку затухание радиосигнала растет с увеличением частоты пропорционально квадрату ее значения, то чем выше используемый диапазон, тем меньше покрытие соты. Поэтому обеспечение сплошного покрытия 5G путем развертывания сети только в новых частотных диапазонах требует большого количества таких сот, что недопустимо увеличивает стоимость строительства и обслуживания инфраструктуры RAN.

Выход состоит в том, чтобы задействовать для сетей 5G комбинацию средних (< 6 ГГц), высоких (> 6 ГГц) и низких частотных диапазонов. В этом случае можно одновременно получить преимущества высоких скоростей и большого покрытия. Такие решения найдены и мобильным операторам хорошо известны.

Внедрение 5G в низкочастотных диапазонах (как правило, занятых LTE-трафиком) осуществляется на базе динамического использования единого пула частотно-временных ресурсов (Dynamic Spectrum Sharing, DSS) для терминалов, имеющих данные для передачи и приема, вне зависимости от стандарта, в котором они работают (LTE или 5G).

DSS поддерживается традиционными производителями RAN – Nokia, Ericsson, Huawei – и в настоящий момент широко внедряется на сетях. По данным, приведенным в отчете 5G Beyond 2020 центра глобальных технологических исследований Omdia, почти половина операторов планирует начать предоставлять коммерческие услуги 5G на базе DSS в течение ближайших двух лет.

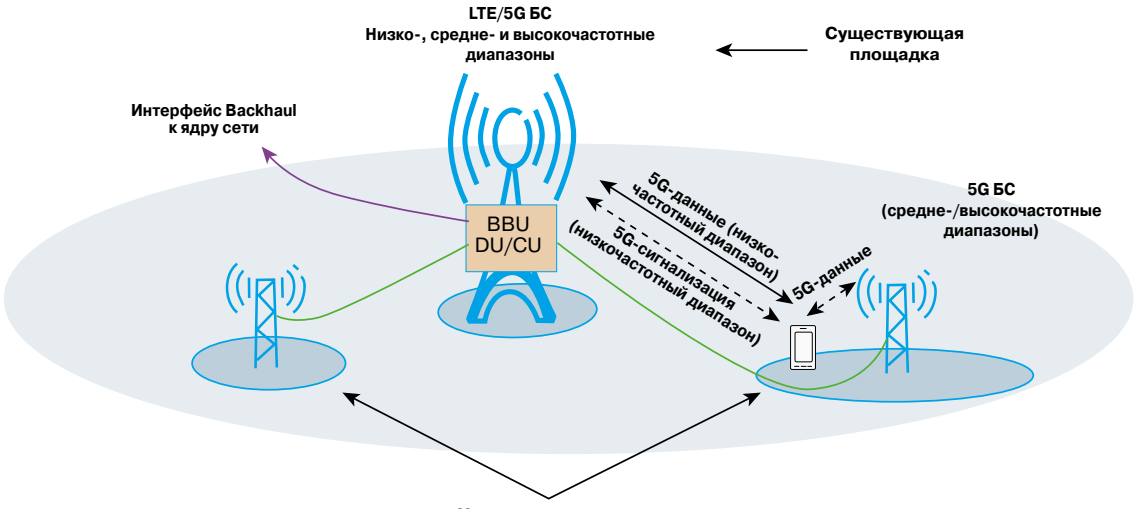
- Основа для комбинации 5G с новыми диапазонами средних и высоких частот – хорошо известное в LTE решение агрегации несущих (Carrier Aggregation, CA). В данном случае речь идет об агрегации 5G-трафика с частотным разделением каналов «вверх/вниз» (Frequency Division Duplex, FDD) в низкочастотном диапазоне и трафика с временны́м разделением каналов «вверх/вниз» (Time Division Duplex, TDD) в новых частотных диапазонах – так называемой междиапазонной агрегации несущих, Inter-band FDD/TDD NR CA. Внедрение Inter-band FDD/TDD NR CA – следующий шаг развития сетей 5G. Запуск первых коммерческих проектов ожидается в I квартале 2021 г.

Целевая архитектура 5G RAN состоит из следующих элементов (рис. 2):

- модули RRH низкочастотных диапазонов (как правило, <2,6 ГГц) для передачи 5G-сигнализации, расширения покрытия в каналах «вверх» и обеспечения мобильности;
- модули RRH более высокочастотных диапазонов для обеспечения высоких скоростей и емкости;
- единый стек цифровой обработки для агрегации несущих низкочастотных и высокочастотных диапазонов, включающий планировщик ресурсов (частота, время, место потребления трафика). Задачей последнего является определение площадок БС, оптимально подходящих для обслуживания каждого терминала для каналов «вверх» и «вниз», выбор их частотных диапазонов для агрегации Inter-band FDD/TDD NR CA, а также временного слота.

В архитектуре RAN сетей 5G можно выделить два типа площадок базовых станций (рис. 3):

- площадки БС с поддержкой 5G в низких диапазонах для обеспечения покрытия. Как правило, это существующие площадки LTE, на которых предоставляются услуги LTE и 5G и установлено оборудование всех диапазонов;
- новые площадки БС с поддержкой 5G в средних и высокочастотных диапазонах, размещенные в местах увеличенного трафика и потребности в высоких скоростях. Как правило, таки-



◀ **Рис. 3. Расположение площадок БС в целевой архитектуре 5G RAN**

ми площадками могут служить столбы освещения, светофоры и т.д., и их намного больше, чем базовых станций покрытия.

Очевидно, централизация цифровой обработки нескольких БС, как показано на рис. 3, даст планировщику ресурсов больше свободы в выборе лучшего сайта для обслуживания каждого терминала, а также повысит эффективность использования и масштабирования вычислительной емкости. Таким образом, целесообразность внедрения в 5G RAN централизованной архитектуры и виртуализации как важного декларируемого качества Open RAN к настоящему времени в отрасли экономически обоснована.

Ключевым становится вопрос о выходе на рынок целевой архитектуры 5G RAN альтернативных поставщиков оборудования Open RAN. С одной стороны, решение CA является моновендорным и не предполагает использования DU разных поставщиков. С другой – в рамках Open RAN поддержка DSS пока не планируется.

Проблема коммерческого внедрения Open RAN в сети радиодоступа состоит не в качестве открытых спецификаций альянса O-RAN, а в том, что на основе этого оборудования невозможно самостоятельно построить целевую архитектуру 5G RAN (нет поддержки DSS, Interband FDD/TDD NR CA). А из-за отсутствия совместимости с решениями традиционных производителей нельзя даже частично участвовать в построении сети и использовать уже реализованную функциональность.

Мультивендорность 5G RAN

5G RAN включает в себя множество интерфейсов, но камнем преткновения мультивендорности является интерфейс Fronthaul между RRH и блоками цифровой обработки BBU/DU (см. рис. 1). В настоящее время традиционные производители применяют закрытые интерфейсы, которые заставляют выбирать RRH и DU одного производителя.

Традиционно используемый для Fronthaul интерфейс CPRI подразумевает передачу оцифрованных отсчетов радиосигнала с ЦАП/АЦП, а вся цифровая обработка концентрируется в BBU/DU/CU. Недостатками CPRI являются рост скорости прямо пропорционально количеству задействованных антенн и ширине радиоканала, а также невозможность агрегации потоков, поскольку частота дискретизации постоянна.

Эти недостатки подтолкнули традиционных производителей RAN к тому, чтобы специфицировать интерфейс eCPRI, который предполагает перенос части низкоуровневых функций цифрового стека DU/CU (часто называемого LowPhy) из централизованного вычислительного пула в RRH либо выделение его в отдельный узел (Interworking Function, IWF-LowPhy), возможно, с его интеграцией в транспортные узлы доступа (Fronthaul gateway, FHG), как показано на рис. 4.

Такой подход за счет уменьшения скорости обмена трафиком с RRH создает предпосылки для того, чтобы агрегировать трафик нескольких RRH, используя зависимость фактической скорости трафика eCPRI от нагрузки соты. В результате снижаются требования к ширине транспортного домена Fronthaul.

Рис. 4. Варианты декомпозиции цифрового стека DU/CU с выделением низкоуровневых функций LowPhy ▼

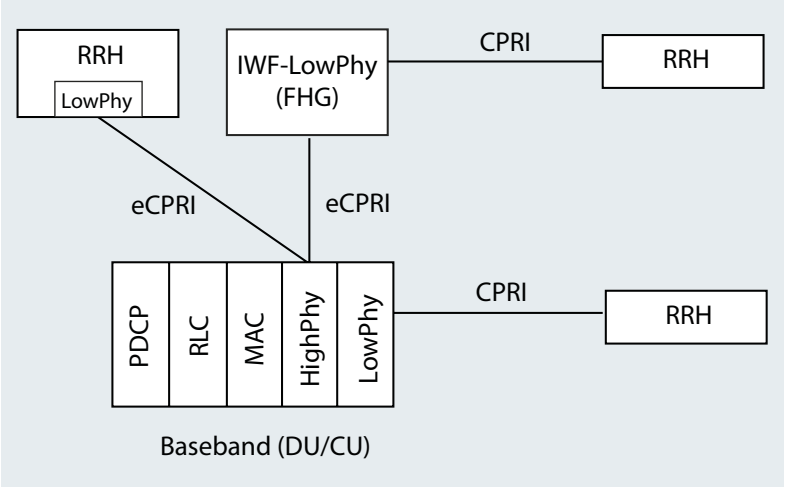
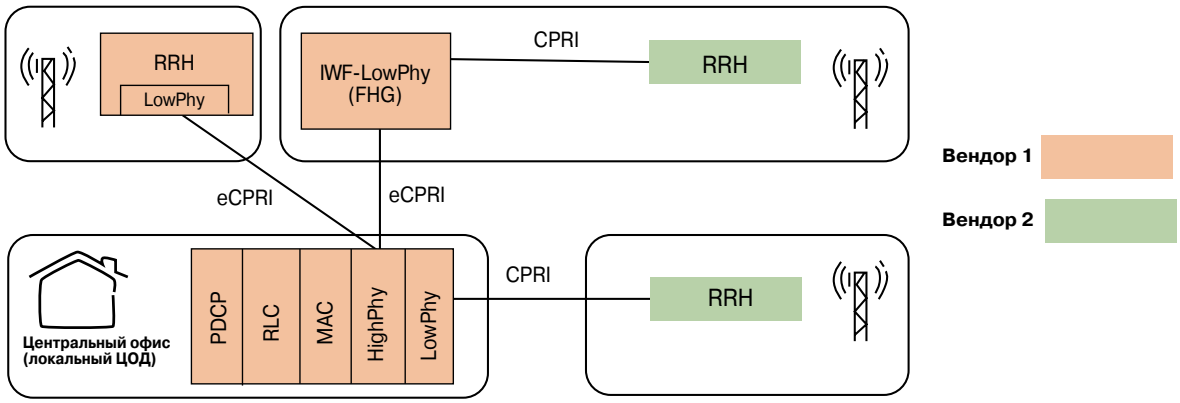


Рис. 5.
Мультивендорное решение построения целевой архитектуры 5G RAN ▶



Полная стандартизация интерфейса eCPRI для межвендорной совместимости позиционируется альянсом O-RAN как один из ключевых элементов для Open RAN.

С позиций сегодняшнего опыта (оставляя за скобками прогресс в области транспортных технологий) видно, что «проблема» ширины транспортного канала Fronthaul несколько преувеличена. Например, емкости одного порта CPRI достаточно для большинства частотных диапазонов и конфигураций 5G RRH*, а поддержка eCPRI при выделении LowPhy из общего пула приводит к увеличению стоимости сетевых узлов. Ожидается, что в сети LTE/5G RAN будут присутствовать оба интерфейса (и CPRI, и eCPRI).

Кроме того, традиционные вендоры обращают внимание на то, что полная стандартизация eCPRI предполагает стандартизацию маппинга символов, которыми кодируется пользовательский трафик, в физически передаваемую в эфир частотно-временную форму. Стандартизация такого маппинга, по их мнению, может стать источником ограничений для совершенствования алгоритмов повышения емкости сети.

Напротив, интерфейс CPRI в части пользовательского трафика является полностью открытым. Специфика его реализации разными производителями ограничена лишь функциями управления и мониторинга RRH, которые не затрагивают пользовательский трафик.

Помимо полной межвендорной совместимости RRH и BBU/DU при использовании CPRI для пользовательского трафика концентрация всей цифровой обработки сигнала в зоне ответственности одного поставщика снимает возможные риски ограничений для любых новых функций в RAN. В настоящий момент, согласно планам альянса O-RAN, предполагается, что разработку алгоритмов и реализацию функций LowPhy должен обеспечить производитель RRH.

Широкое использование интерфейса CPRI позволяет разорвать моновендорность целевой архитектуры 5G RAN (рис. 5) и внедрять решения новых производителей при гарантии полноты и качества использования любой функциональности RAN.

Простота обеспечения межвендорной совместимости при использовании CPRI замечена отраслью. Решения RAN на базе CPRI с разными поставщиками RRH и BBU/DU широко применяются ведущими операторами и ключевыми участниками инициативы Open RAN (например, Verizon и AT&T). Кроме того, при строительстве сети Rakuten (Япония) успешно задействовался интерфейс eCPRI с вынесенным узлом IWF-LowPhy и RRH стороннего производителя.

Такой подход позволяет операторам усилить конкуренцию и получить более выгодные коммерческие условия, а также иметь возможность оперативно заменить одного поставщика на другого при возникновении технологических рисков. Последнее позволит гарантировать своевременное развертывание сети и избежать возникшей однажды ситуации, когда головным поставщиком при выборе компонентной базы BBU/DU были допущены просчеты, которые привели к срыву поставки необходимых коммерческих решений. В настоящее время мобильная сетевая инфраструктура RAN российских операторов от подобных технологических рисков не защищена.

Внедрение Open RAN на российском рынке

Обеспечение межвендорной совместимости при использовании интерфейса CPRI достигается за счет раскрытия спецификации CPRI произ-

* Можно показать, что с точки зрения минимизации количества портов RRH использование eCPRI необходимо только в средних частотных диапазонах и только для mMIMO (т.е. конфигураций 16T/16R, 32T/32R, 64T/64R). При этом доля RRH с mMIMO в этих диапазонах оценивается, по данным опроса операторов, проведенного Heavy Reading и 5G Americas, не более чем в 50% числа существующих сайтов. Для других частотных диапазонов и конфигураций RRH достаточно одного порта даже при использовании CPRI (до 25 Гбит/с).

водителями RAN для других поставщиков. Как было показано выше, эта мера успешно применяется на мобильном рынке на уровне взаимодействия операторов с поставщиками. Однако российские операторы не имеют сильных переговорных позиций с поставщиками RAN.

Предлагается законодательно закрепить обязательность раскрытия спецификации CPRI для других поставщиков как условие применения оборудования на сетях РФ. Это позволит максимально ускорить переход на открытую архитектуру RAN в сетях всех российских операторов и разрешить описанные выше противоречия при внедрении Open RAN для всех заинтересованных сторон.

Такая мера позволит мобильным операторам уже на начальном этапе строительства сетей 5G получить более выгодные коммерческие предложения за счет усиления конкуренции между традиционными производителями. Возможность замены оборудования (RRH или BBU/DU/CU) одного традиционного поставщика на оборудование другого поможет минимизировать технологические риски, т.е. обеспечить устойчивость сетевого решения к замене оборудования при сохранении предоставления услуг на всей площади покрытия.

Также у операторов появится возможность использовать отдельные элементы продуктовой линейки отечественных производителей по мере их коммерческой готовности, что будет способствовать уменьшению задержки развертывания сетей 5G в РФ без каких-либо рисков в части ограничения потребительских качеств для абонентов и конкурентоспособности операторов.

Возможность вывода отдельных отечественных продуктов (RRH, DU, BBU, CU) на рынок и их коммерческое внедрение без необходимости ожидать создания полной продуктовой линейки гарантирует более быстрый возврат государственных инвестиций и ускорит переход на отечественную продукцию.

Подтвердив качество межвендорной совместимости с оборудованием традиционных поставщиков на российском рынке, отечественные производители получат возможность расширить каналы продаж своей продукции за счет выхода на международный рынок. Хорошо известно, что в мобильной индустрии не хватает поставщиков радиочасти для базовых станций (радиомодулей RRH), способных организовать крупносерийное производство. Производственные мощности российских предприятий позволяют занять эту нишу.

■■■

Внимание к проблемам демонополизации рынка оборудования RAN и поддержка собственной промышленности – объективная тенденция во многих странах. Можно лишь приветствовать решение российских государственных органов об использовании «радиоэлектронных средств только российского происхождения».

Однако, если эти волевые решения не будут подкреплены «тонкими настройками», то возникнет большой риск, что внедрение 5G на российском рынке сведется к «квесту» попадания традиционных производителей RAN в Единый реестр российской радиоэлектронной продукции, результатом чего станет большая задержка развертывания сетей 5G в России. Рынок мобильной связи для отечественной промышленности останется ограниченным узкоспециализированными дотационными проектами (например, предоставления 5G в малонаселенных районах или устранения цифрового неравенства), которые не позволят обеспечить экономическую и функциональную конкурентоспособность отечественных решений.

Преимущества предлагаемого подхода: возможность применения на всех этапах строительства 5G RAN, устранение рисков межвендорной несовместимости, гарантия качества предоставляемых услуг и перспективы выхода отечественной промышленности на международный рынок. Последнее является как уникальной возможностью, так и важным фактором высокой экономической конкурентоспособности, обоснованием целесообразности государственных инвестиций в разработку.

Понятно, что «тонкие настройки» в технической области не сводятся только к межвендорной совместимости RRH и BBU/DU. Так, если важнейшим критерием внедрения 5G будет являться безопасность, то одним из приоритетов (при всей важности средних частотных диапазонов 3,4–3,8 ГГц) должна стать первоочередная разработка и переход на использование отечественных RRH низких частотных диапазонов, которые помимо переноса пользовательского трафика будут задействованы как среда для передачи 5G-сигнализации во всей сети (см. рис. 2). Тогда даже при наличии в сети RRH более высоких диапазонов зарубежного производства и утере контроля над ними (например, в случае прекращения техподдержки) услуги будут предоставляться на всей площади покрытия благодаря использованию отечественного оборудования.

Есть и другие важные задачи, ждущие своего решения. Требуется кропотливая профессиональная работа по формулированию технических требований к разрабатываемой отечественной продукции, которые позволят ей стать конкурентоспособной. Также необходимо создать условия для вывода продукции отечественных производителей на коммерческий рынок мобильной связи. ИКС

Под знаком Digital

События 2020 г. ускорили цифровизацию всех сторон нашей жизни и деятельности. О повышении значимости цифровых технологий, развитии рынка инженерной инфраструктуры и ЦОДов – Наталия Макарочкина, старший вице-президент подразделения Secure Power компании Schneider Electric в регионе International.

– Насколько события 2020 г. ускорили внедрение и использование цифровых технологий в экономике?

– Все происходящее в этом году показывает, что снижение зависимости от человеческого фактора и уменьшение участия человека в ключевых этапах бизнес-процессов возможно только при условии цифровой трансформации. В качестве примера можно привести финансовый сектор, где юридически значимый электронный документооборот позволил избежать физического присутствия части сотрудников для обработки и подписания бумажных документов. В промышленном секторе наличие автоматизированных систем диспетчерского управления дало возможность удаленно контролировать состояние оборудования и технологических процессов. Также мы видим активное развитие онлайн-платформ во многих, в том числе консервативных, сегментах – по прогнозам компании Arcadier, в течение следующих пяти лет 75% B2B-закупок будет осуществляться через торговые онлайн-площадки.

Главное то, что в основе всех этих систем лежат цифровые технологии. Поэтому активное внедрение подобных систем под воздействием событий 2020 г. обусловило повышение спроса как на соответствующее ИТ-оборудование, так и на обеспечивающую его работу инженерную инфраструктуру. Этот же тренд приводит к тому, что мы видим все более ярко выраженную специализацию ЦОДов по трем основным направлениям: укрупнение центральных ЦОДов, создание опорных региональных ЦОДов и активное развитие периферийных вычислений, разворачиваемых непосредственно в том месте, где создаются первичные цифровые данные, для повышения эффективности их обработки.

– Что значит «цифровизация» для вас? В чем суть цифровых преобразований, проходящих в компании?

– Перемены затронули и Schneider Electric – мы были хорошо подготовлены к изменению режима работы сотрудников благодаря уже внедренным цифровым решениям, онлайн-сервисам поддержки внутренних бизнес-процессов и средствам виртуальной коллаборации, а также, что немаловажно, развитой культуре удаленной работы и взаимодействия сотрудников.

Тем не менее мы в сжатые сроки значительно нарастили мощности существующих систем, внедрили новые, более эффективные цифровые средства удаленного взаимодействия, провели обучение сотрудников работе с отдельными системами и наиболее эффективному выстраиванию процессов в новой реальности, когда привычное «физическое» взаимодействие людей как внутри компании, так и с партнерами и заказчиками может быть ограничено.

Примером успешной цифровой трансформации может служить и перевод в полностью цифровой формат нашего ключевого ежегодного мероприятия – Innovation Summit. Благодаря инновационному подходу мы смогли совместить преимущества «физического» мероприятия – живое общение, демостенды, виртуальные тестирования и лаборатории – с гибкостью и доступностью цифрового формата.

– Мы наблюдаем стремительное развитие сервисной модели во всех областях. Насколько она применима к тем решениям, которые предлагает Schneider Electric?

– Schneider Electric обладает развитой партнерской экосистемой, куда входят, в частности, сервис-провайдеры, в том числе в области решений для инженерной инфраструктуры. Мы предоставляем им необходимые инструменты на базе цифровой платформы EcoStruxure, которые позволяют результативно реализовать сервисную модель благодаря тому, что, с одной стороны, повышают эффективность бизнеса партнеров за счет гибкого подхода к оказанию цифровых услуг по подписке, а с другой – повышают уровень сервиса для их заказчиков с помощью централизованного мониторинга и предиктивной аналитики состояния установленного оборудования, обеспечения оперативной инвентаризации и контроля инцидентов безопасности.

Согласно международным исследованиям, только 27% поставщиков управляемых услуг предоставляют сервис контроля электроснабжения. И большая часть из них делают это только в режиме «вкл.» или «выкл.». Возможности, которые мы предлагаем партнерам, значительно шире, именно поэтому несколько сотен партнеров присоединились к использованию нашей платформы только за этот год.

– Переход на «удаленку» выявил важность современных систем автоматизации, в том числе в части эксплуатации ЦОДов. Можно ли минимизировать участие человека в этих процессах?

– Два ключевых направления для Schneider Electric – это продукты, а также ПО и сервисы. Их объединяет именно цифровизация, позволяющая осуществить их интеграцию в единую систему, создавая синергический эффект. Благодаря тому, что практически все наши продукты являются подключаемыми, наши заказчики могут осуществлять удаленный мониторинг всех ключевых узлов инфраструктуры – всей цепочки энергоснабжения ЦОДа, холодоснабжения и других критически важных инженерных систем и систем безопасности. Соответственно, мы позволяем опе-

ративно определить и устранить причину нештатной ситуации в случае ее возникновения.

Однако сейчас мы идем еще дальше – благодаря анализу накопленных больших данных об оборудовании и произошедших событиях мы можем не только говорить о его текущем состоянии, но и делать прогноз с целью предотвращения выхода из строя отдельных компонентов. Это дает возможность перейти от реактивных действий к проактивным, а предотвращение аварий, как известно, намного менее затратно, чем их устранение.

– ИТ эволюционируют от распределенной модели к централизованной и снова к распределенной. В чем современные периферийные узлы принципиально отличаются от старых серверных?

– Действительно, мы наблюдаем очередной виток развития принципов построения ИТ – переход к децентрализованной иерархической распределенной архитектуре, но уже на новом уровне. Принципиальное отличие в том, что теперь это не отдельные независимые узлы, а элементы единой информационной системы. Соответственно влияние отказа отдельного узла более не ограничивается только этим узлом, а распространяется на всю систему и эффективность ее работы в целом.

Поэтому необходимы единый комплексный подход к архитектуре вычислительных узлов всех уровней, который позволит повысить эффективность обслуживания и эксплуатации, и единые требования к их отказоустойчивости или уровню резервирования. И наконец, как уже отмечалось, важна централизованная система удаленного мониторинга и контроля состояния ключевых компонентов, параметров среды и инцидентов, связанных с безопасностью.

– Сегодня заказчики все чаще хотят получить все им необходимое из «одного окна». Чтобы обеспечить это, многие поставщики формируют широкие экосистемы. Как подобная работа ведется в Schneider Electric?

– Термин «экосистема» хорошо описывает подход Schneider Electric. Здесь я могу выделить два аспекта: во-первых, технологии. Мы развиваем различные технологические направления, адаптируем наше предложение, чтобы максимально удовлетворить потребности заказчиков с учетом специфики отраслей и даже отдельных компаний. Это энергоснабжение и энергоэффективность, цифровые средства автоматизации, облачные решения и инженерная платформа для информационных и технологических систем. Таким образом мы формируем единую комплексную экоструктуру подключенных устройств, объединенную общей системой мониторинга и управления, аналитикой, приложениями и сервисами.

Второй аспект – экосистема партнеров. Мы не ограничиваемся только работой с ИТ-интеграторами, мы активно сотрудничаем с электротехническими партнерами, сервис-провайдерами, компаниями, специализирующимися на IoT и цифровой трансформации, консалтинговыми и проектными организациями. Экспертиза наших партнеров позволяет сформировать исчерпывающее предложение для разных сегментов бизнеса: коммерческих дата-центров, промышленных, нефтегазовых предприятий, медицины и многих других отраслей.

– Schneider Electric известна как поставщик комплексных инженерных систем. А что с ИТ? Могут ли заказчики сегодня получить полностью готовый продукт, например микроЦОД, укомплектованный как инженерными, так и ИТ-системами?

– Еще одна сторона нашей экосистемы – партнерские альянсы с ведущими производителями ИТ-оборудования, такими как Dell, HPE, Cisco. Мы высоко ценим наши отношения с партнерами, их экспертизу и не стремимся конкурировать с ними. Однако, если заказчику требуется интегрированное комплексное решение от вендора, охватывающее инженерные и ИТ-системы, мы можем предоставить ему инфраструктуру с предустановленным оборудованием наших альянс-партнеров. У нас уже есть реализованные в России проекты, когда заказчик получил законченное plug-and-play решение для периферийных вычислений, включающее в себя в том числе активное оборудование. Более того, у нас есть специальный инструмент Local Edge Configurator, который мы специально разработали для такого рода проектов и задач. На данный момент к этому инструменту имеют доступ наши партнеры, которые могут собрать полноценное решение и проверить все компоненты на совместимость.

– Schneider Electric уделяет большое внимание энергоэффективным технологиям. Но соответствующие решения часто дороги. А в нынешних условиях заказчики стремятся минимизировать CAPEX. Скажется ли это на развитии энергоэффективных систем?

– Повышение энергоэффективности предприятия и уменьшение счета за электроэнергию не всегда требует CAPEX, возможно обойтись и операционными расходами. Например, мы можем предложить с помощью оптимизации бизнес-процессов, настройки и взаимно согласованной работы отдельных инженерных систем повысить их производительность и эффективность, не устанавливая дополнительного оборудования. С другой стороны, вложения в энергоэффективные технологии положительно влияют на имидж и репутацию организации. Также некоторые страны поощряют импорт товаров, произведенных с соблюдением экологических норм, поэтому внедренные энергоэффективные технологии могут помочь компании открыть новые рынки сбыта.

Мы ожидаем, что энергоэффективные, более экологичные технологии будут развиваться и становиться все более популярными и, как следствие, доступными. Schneider Electric не только является надежным партнером для заказчиков в области цифровой трансформации, устойчивого развития и эффективности. Мы сами активно внедряем подобные технологии на своих предприятиях и стремимся соответствовать высоким стандартам экологичности.

Wi-Fi 6 и 5G: от соперничества к сотрудничеству

Николай Ефимов, технический менеджер в России и странах СНГ, Siemon

Сочетание технологий Wi-Fi 6 и 5G позволит создавать как протяженное, так и локальное покрытие, обеспечивающее высокоскоростной беспроводной доступ. Но для эффективной работы оборудования этих сетей требуются высокопроизводительные кабельные системы.

Недавно был опубликован стандарт 802.11ax, описывающий новое поколение приложений Wi-Fi, более известное как Wi-Fi 6. С появлением и постепенным распространением сетей 5G могло сложиться впечатление, что эти две технологии конкурируют друг с другом. Однако на самом деле это не так. Каждая из технологий нашла свою нишу в современном цифровом мире, они прекрасно сосуществуют и дополняют друг друга.

Путаница и неразбериха

Предшественниками систем Wi-Fi 6 были решения Wi-Fi 5, работающие в полосе 5 ГГц. Они широко распространились и последние пять лет демонстрировали устойчивый рост. Одновременно в телекоммуникационной отрасли активно шло обсуждение решений 5G для мобильной связи, и это привело к путанице – многие стали считать, что речь идет о развитии одной и той же технологии. Когда же Институт инженеров по электротехнике и электронике (IEEE) выпустил стандарт Wi-Fi 6 (802.11ax), некоторые подумали, что это решение лучше, чем 5G. Теперь же появилась еще и технология Wi-Fi 6E (802.11ax), предусматривающая использование полосы 6 ГГц в дополнение к частотам 2,4 ГГц и 5 ГГц, на которых работают решения Wi-Fi 6.

Сколько бы стандартов и нормативных документов ни выходило в свет, надо понимать, что решения 5G (новое поколение систем сотовой связи) и Wi-Fi (для создания беспроводной локальной сети) – совсем не одно и то же! Технология 5G относится к гражданской мобильной связи, рассчитана на многокилометровые зоны покрытия и призвана поддержать будущие системы беспилотного транспорта, отслеживания автомобилей и других средств передвижения, а также транспортировки грузов и т. п. Решения Wi-Fi должны предоставлять высокоскоростной доступ к локальным сетям и обеспечивать выход в интернет на объектах небольшой протяженности, в кампусах и зданиях. Их задача – поддержать бизнес-приложения и реализацию концепции интернета вещей.

Лицензируемые частоты для сотовой связи и нелицензируемые – для Wi-Fi

5G – обозначение пятого поколения технологий для сетей мобильной связи. Сотовые сети 4G LTE и 5G работают в лицензируемых диапазонах радиочастотного спектра: только компания, получившая соответствующую лицензию, имеет право работать на определенных частотах. Правда, предполагается, что системы 5G займут и некоторые нелицензируемые полосы частот – их смогут использовать операторы сетей 5G (и не только) для расширения существующих сетей и запуска новых.

Стандарты и частоты Wi-Fi

- Wi-Fi 4 (802.11n): 2,4 или 5 ГГц
- Wi-Fi 5 (802.11ac): только 5 ГГц
- Wi-Fi 6 (802.11ax): 2,4 или 5 ГГц
- Wi-Fi 6E (802.11ax): 2,4, 5 и 6 ГГц

Сигналы Wi-Fi передаются через беспроводные точки доступа в частных сетях на ограниченное расстояние. Выход в интернет происходит через интернет-провайдеров, предоставляющих такие услуги частным сетям. В отличие от лицензируемых частот сотовой связи, выделяемых конкретному мобильному оператору, полосы 2,4, 5 и 6 ГГц, в которых работают разные поколения приложений Wi-Fi, нелицензируемые, и использовать их может кто угодно.

Важно понимать, что Wi-Fi 6E – это не новый беспроводной протокол, а расширение Wi-Fi 6, предусматривающее предоставление приложениям дополнительной полосы 6 ГГц.

Скорости передачи в сетях Wi-Fi и в системах сотовой связи

Как в сетях Wi-Fi, так и в сотовых сетях 4G или 5G скорость передачи данных зависит от того, к какой сети подключился пользователь, каким устройством он располагает и сколько других пользователей одновременно с ним подключены к той же самой сети.

Максимальная скорость передачи в ранних сотовых сетях 4G составляла 150 Мбит/с, однако на одного пользователя приходилось в среднем всего 10 Мбит/с. Сети 4G LTE и 4G LTE-A способны обеспечить скорости от 300 Мбит/с до 1 Гбит/с, при этом в среднем пользователю предоставляется скорость загрузки около 15 Мбит/с. Сети LTE были призваны преодолеть ограничения, свойственные сетям 4G; они перевели передачу данных в системы на основе интернет-протокола и позволили передавать пакеты данных большего размера и с меньшими задержками.

В сотовых сетях 5G используются высокочастотные радиосигналы, потенциально способные обеспечить скорость передачи от 1 до 10 Гбит/с. Скорость загрузки у одного пользователя в среднем будет достигать 50 Мбит/с при уменьшенном времени ожидания. Однако более высокая частота радиоволн в сетях 5G подразумевает зону покрытия меньшего радиуса, чем у частот, используемых сегодня антеннами 4G. Приходится проектировать соты меньшего размера и размещать ретрансляторы ближе к пользователям и устройствам. В основаниях таких антенно-мачтовых сооружений стали размещать периферийные центры обработки данных.

В сетях Wi-Fi скорости передачи выше, чем в сотовых, однако в них нужно больше внимания уделять ширине и количеству каналов, доступных в той или иной полосе частот, способности передавать и принимать сигналы через множественные антенны (используются пространственные потоки), схеме кодирования и распределению (разделению) полосы пропускания в соответствии с потребностями. Системы Wi-Fi 4 с четырьмя пространственными потоками теоретически способны поддерживать скорость передачи данных на уровне 576 Мбит/с (144 Мбит/с на каждый поток). Сети Wi-Fi 5 с восемью пространственными потоками имеют теоретический максимум скорости 6,93 Гбит/с (866 Мбит/с на один поток), а системы Wi-Fi 6/6E с теми же восемью потоками, но более эффективной схемой кодирования обеспечат максимальную скорость 9,61 Гбит/с (1,2 Гбит/с на каждый поток).

Поскольку полоса пропускания и количество пространственных потоков могут быть разными и могут применяться многопользовательские механизмы передачи сигналов, системы Wi-Fi 5, Wi-Fi 6 и Wi-Fi 6E настраиваются очень гибко. На практике нижние зоны в полосе пропускания выделены для носимых устройств с ограниченной емкостью батареи (смартфонов), средние диапазоны предназначены для ноутбуков, а верхний диапазон полосы пропускания обслуживает специализированное оборудование и уличные решения, где плотность размещения устройств заведомо меньше, чем внутри помещений (см. таблицу).

Требования к кабельным системам

Системы Wi-Fi будут эффективно работать только в том случае, если к беспроводным точкам доступа подведена высокопроизводительная кабельная инфраструктура. При проектировании и монтаже кабельных систем, к кото-

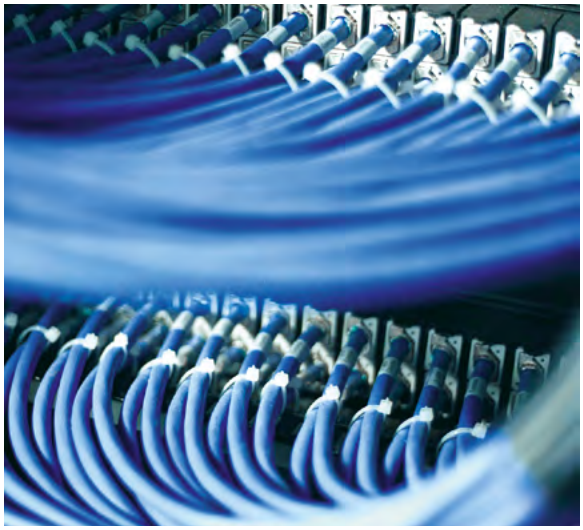
Конфигурации и сценарии обслуживания систем Wi-Fi 5 и Wi-Fi 6/6E ▼

Канал	Число пространственных потоков	Максимальная скорость		Обслуживаемые устройства и приложения
		Wi-Fi 5	Wi-Fi 6/6E	
Решения «первой волны»				
80 МГц	1	433 Мбит/с	540 Мбит/с	Двухполосные смартфоны, планшеты, носимые трубки VoIP
80 МГц	3	1,3 Гбит/с	1,6 Гбит/с	Мощные ноутбуки, цифровая кинематография
Решения «второй волны»				
80 МГц	2	867 Мбит/с	1,1 Гбит/с	Нетбуки, ноутбуки средней производительности
160 МГц	3	2,6 Гбит/с	3,6 Гбит/с	Мощные ноутбуки, цифровая кинематография
Возможные конфигурации в будущем				
160 МГц	4	3,5 Гбит/с	4,8 Гбит/с	Уличные системы, зоны с малым охватом
160 МГц	8	—	9,61 Гбит/с	Специализированные устройства

рым затем будут подключаться точки доступа в корпоративных системах Wi-Fi 6/6E, нужно учитывать целый ряд важных рекомендаций.

- К каждой точке доступа должны быть подведены минимум два сегмента категории 6A (или категории 7A), обеспечивающих скорость передачи 10 Гбит/с и поддерживающих агрегирование восходящих каналов 2,5G/5G/10GBASE-T.
- Для создания восходящих каналов повышенной производительности для систем Wi-Fi 6 и Wi-Fi 6E следует устанавливать многомодовые оптические магистрали с производительностью не менее 25 Гбит/с.
- Для обеспечения удаленного питания устройств Wi-Fi 6 (например, PoE Type 2 мощностью 30 Вт) следует создавать экранированные кабельные системы, поскольку они лучше противодействуют росту температуры внутри кабельных пучков, а значит, надежнее поддерживают требуемые характеристики передачи. Экранированные системы категорий 6A или 7A обеспечивают высокую стойкость к повышенным температурам и рассчитаны на поддержание характеристик передачи при температурах до 75°C.
- В системах следует применять коммутационные компоненты, соответствующие требованиям стандарта IEC 60512-99-001. Это позволит избежать выгорания контактов в сетевых устройствах и портах при отключении вилок, когда используется удаленное питание PoE.
- При проектировании кабельных систем необходимо применять зональный подход (рекомендуется сетчатая структура), поскольку он облегчает установку дополнительных точек доступа и изменение конфигурации зон обслуживания. Зональный подход обеспечит гибкость системы и возможность ее использования на многие годы вперед.

Применение систем 5G расширяется. Их развертывание будет сопровождаться установкой периферийных центров обработки данных, а в них тоже используется кабельная инфраструктура. Ее характеристики имеют большое значение для эффективной работы систем 5G. В периферийных ЦОДах следует устанавливать высокопроизводительные медные и волоконно-оптические кабельные системы – кабели и коммутационные компоненты. Медные кабельные системы категории 6A способны поддерживать скорость 10 Гбит/с, категории 8 – скорости 25 и 40 Гбит/с. Для передачи



больших объемов данных с высокой скоростью между единицами активного оборудования (между коммутаторами, от коммутаторов к серверам, от коммутаторов к устройствам хранения) будут широко применяться высокоскоростные шнуры прямого подключения (High-Speed Interconnect solutions) небольшой длины. Эти решения особенно эффективны для периферийных ЦОДов, поскольку в них оборудование размещается в одной и той же или в соседних стойках. Высокоскоростные шнуры выпускаются в разных вариантах – медные шнуры прямого подключения (Direct Attach Copper Cables) и активные оптические шнуры (Active Optical Cables) – и поддерживают скорости передачи от 10 до 100 Гбит/с. Их использование позволяет снизить расходы, обычно связанные с трансиверными решениями, и обеспечивает более высокую надежность, поскольку точек соединения – потенциальных точек сбоя – становится меньше.

В периферийных ЦОДах на малой площади располагается большое количество медных точек подключения, и ими нужно грамотно управлять. Высокоплотные решения для кабельных систем категории 6A/класса EA прекрасно подходят для использования на таких объектах за счет своей компактности. Для волоконно-оптических систем также существуют высокоплотные решения: оптические шкафчики высокой плотности при высоте 1U способны вместить 144 волокна для коннекторов LC или 864 волокна для интерфейсов MTP. Высокая плотность портов сопровождается удобством и простотой доступа к каждому подключению; в шкафчиках хорошо продумана укладка кабелей и шнуров.

Для подключения периферийных ЦОДов к центрам колокации, облачным дата-центрам, сверхбольшим ЦОДам и узлам связи лучше всего подходят волоконно-оптические магистрали, обеспечивающие пропускную способность на уровне 400 Гбит/с или выше. ИКС

В ближайшее десятилетие альтернативы ДГУ нет

Дизель-генераторы – основа систем гарантированного электропитания ЦОДов, обеспечивающих им автономную работу при длительных отключениях электричества. О развитии и перспективах этих решений – Ален Десессард, директор московского офиса компании SDMO (входит в состав KOHLER).

– Какой основной тренд в развитии систем бесперебойного и гарантированного электропитания ЦОДов вы можете выделить?

– На мой взгляд, главный тренд – переход к стандартизированным решениям с высокой степенью заводской готовности. Заказчики хотят иметь типовые системы, которые можно использовать для различных проектов. Это позволяет им лучше контролировать технические риски и существенно сократить сроки реализации проектов.

В случае дизель-генераторных установок (ДГУ) этот тренд проявляется в использовании модульных решений. Модулем является ДГУ на базе контейнера. Такой модуль (контейнер) можно оперативно доставить на площадку, быстро и без проблем подключить к другим системам, а для наращивания мощности объекта добавлять модули по мере необходимости. Кроме того, мы предлагаем модули для звукоизоляции, дымоотвода и т.д., которые дополняют базовый модуль ДГУ.

– ДГУ и раньше поставляли в контейнерах. В чем отличие нового, модульного подхода?

– Раньше ДГУ все же чаще устанавливали в помещении, а не в контейнере. По крайней мере в Европе большинство инсталляций ДГУ для ЦОДов были внутри зданий. Каждая установка ДГУ в здании – это отдельный проект, в котором надо предусмотреть системы отвода тепла, выхлопа, звукоизоляции и т.д. Для каждого здания необходимо свое проектирование, что долго и дорого.

Контейнер можно быстро установить там, где требуется. А новое поколение модульных решений – это типовые, полностью готовые к эксплуатации системы, в которых все уже предусмотрено. Такие решения подходят для всех типов дата-центров, будь то гипер-ЦОДы, корпоративные или традиционные коммерческие ЦОДы для предоставления услуг colocation – всюду используются, по сути, одни и те же технические решения, меняются только их мощность и физические размеры.

– Каковы мощность и размер таких модулей? Что, например, вы можете предложить для небольших объектов, таких как edge-ЦОДы?

– В нашем понимании edge-ЦОД – это объект мощностью до 5 МВт. Для подобных ЦОДов мы предлагаем модульные ДГУ мощностью 500–1500 кВА. Они устанавливаются с защитным кожухом или в 20-футовые контейнеры.

– Но есть edge-ЦОДы буквально на несколько стоек, суммарной мощностью несколько десятков киловатт. Для таких проектов у вас есть решения?

– У нас накоплен большой опыт поставок дизель-генераторов небольшой мощности – от 20 до 500 кВт – для телекоммуникационных, банковских и других заказчиков. Эти решения могут с успехом использоваться и для гарантированного электропитания малых ЦОДов.

В нашем продуктовом портфеле есть дизель-генераторы мощностью от 9 до 4500 кВА. Кстати, в настоящее время установка на 4500 кВА – это самый мощный ДГУ в мире.

– ДГУ – довольно консервативные системы. Какие инновации внедрены в них за последние годы?

– Да, дизель-генераторы существуют давно, но сама технология не стоит на месте. За последние годы огромные изменения произошли в конструкции установок, значительно снижены выбросы и шум, улучшены другие характеристики. Два основных направления, в которых работают наши инженеры, – это уменьшение расхода топлива и уровня вредных выбросов.

Одна из наиболее совершенных линеек ДГУ – линейка KD Series, выпущенная нами на рынок

в 2016 г. на базе двигателей Kohler. Это самые компактные решения с низким потреблением топлива и высокой эффективностью работы. Мощность ДГУ серии KD составляет от 800 до уже упомянутого рекордного значения 4500 кВА.

Большое внимание наши разработчики уделяют развитию средств автоматизации. Современные ДГУ снабжены множеством датчиков, позволяющих удаленно контролировать основные параметры, например, температуру двигателя, расход и уровень топлива, величину нагрузки и пр. Возможности удаленного мониторинга отлично показали себя в условиях пандемии, когда многие заказчики старались сократить штат сотрудников, находящихся непосредственно на объекте.

Отмечу еще одно направление совершенствования ДГУ. Если 10 лет назад на то, чтобы дизель-генератор гарантированно завелся и вышел на штатный режим работы, проектировщики систем бесперебойного и гарантированного электропитания обычно отводили несколько минут, то сегодня для этого достаточно менее 30 с. Таким образом, приобретая качественный ДГУ, заказчик может существенно снизить время автономной работы от аккумуляторных батарей, следовательно, сократить расходы на эти дорогостоящие элементы.

– В проектах строительства ЦОДов у заказчиков все более востребована комплексная инженерная инфраструктура от одного поставщика. ДГУ стоят особняком, поскольку их не производит ни один крупный поставщик такой инфраструктуры. Как вы строите партнерства с такими компаниями?

– Если рассматривать модульные решения ДГУ, о которых я говорил раньше, то их важное свойство – упрощенное подключение к другим системам, например к ИБП, причем вне зависимости от того, какая компания их производит. Вообще говоря, для поставщиков статических ИБП мы – естественный партнер, поскольку именно связка «ИБП + ДГУ» является основой системы бесперебойного и гарантированного электропитания большинства ЦОДов. Такие комплексы доказали свою надежность и эффективность десятилетиями успешной работы на сотнях и даже тысячах объектов.

– А поставщики динамических ИБП, в составе которых имеются ДГУ, вам конкуренты или партнеры?

– Когда они используют наши ДГУ в составе своего решения – партнеры, а когда в проекте динамический ИБП соревнуется со связкой «статический ИБП + ДГУ» – конкуренты. Кстати, наши ДГУ задействует, например, в своих динамических ИБП компания Piller.

В отношении динамических ИБП хотел бы отметить разницу между ситуацией в Европе и в России. Такие ИБП были популярны в Европе лет десять назад. Но сейчас они постепенно «выходят из моды». Дело в том, что это технически более сложная и дорогая в обслуживании система по сравнению с комплексом «статический ИБП + ДГУ». В Европе все меньше клиентов выбирают динамические ИБП. В России же на данный момент они активно используются, особенно крупными ЦОДами. Думаю, ситуация будет меняться.

– Не могу не спросить про трудности текущего момента. Как вам работается в условиях пандемии?

– Пришлось менять организацию работы, процесс производства. Мы увеличили дистанцию между рабочими на наших заводах, которые расположены во Франции. Офисные работники перешли на удаленный режим. Уже принято решение, которое позволит им и после окончания пандемии три дня в неделю работать из дома.

– Насколько увеличилось время поставки ДГУ заказчикам в Россию?

– Здесь ничего не изменилось. Большой склад во Франции и склад нашего местного партнера АО «ГрандМоторс» позволяют поставлять типовые решения за две недели. Кстати, модульный подход существенно упростил логистику. Если надо специально изготавливать ДГУ под конкретный проект, то тогда заказчик получит его через 6–12 недель.

– SDMO хорошо известна российским специалистам как производитель качественных ДГУ. Что еще интересного вы можете рассказать о компании?

– Основанная в 1966 г. в Бресте (Франция) компания с 2005 г. входит в состав американской корпорации Kohler. В портфеле наших решений помимо ДГУ имеются газопоршневые установки относительно небольшой мощности – до 400 кВт. Но главная наша специализация – это, конечно, дизель-генераторы. В России наши ДГУ используются на большом числе различных объектов. Назову, в частности, энергокомплексы на 12 МВт для стадионов World Cup 2018, на 5,7 МВт для медицинского центра «Новомосковский» (более известного как «Коммунарка»). Если говорить о ЦОДах, то наши ДГУ установлены на объектах «Ростелекома» и «Вымпелкома», в стадии реализации проект с Selectel.

– Анализируя ряд факторов (ужесточение экологических требований, развитие альтернативных решений и пр.), некоторые эксперты прогнозируют, что ДГУ в ЦОДах будут использоваться меньше. Согласны ли вы с этим мнением?

– Вопросы экологии стоят остро, особенно в Европе. Тем не менее, на наш взгляд, в течение 10 лет ДГУ останутся незаменимыми источниками автономного электропитания большинства объектов, включая ЦОДы. Дело в том, что новые технологии и альтернативные решения – топливные элементы, водородные генераторы и пр. – еще очень незрелые. Потребуется не один год для их совершенствования и вывода на уровень массового применения.

– А что будет после 2030 г.?

– Сегодня никто не скажет точно, какая технология придет на смену существующим. Если же говорить об альтернативных источниках, то нам интересно развитие топливных элементов. Видим здесь перспективу.

Но пока технологии ДГУ нужны, я бы даже сказал, жизненно важны. Заменить их сейчас просто нечем. Нет другой такой технологии, которая обеспечила бы столь высокую надежность и низкие эксплуатационные расходы при практически неограниченной возможности генерации электроэнергии.

KOHLER. SDMO.
Ален ДЕСЕССАРД,
директор филиала SDMO в Москве
alain.desessard@kohler.com

Адиабатика: какую систему выбрать?

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

Благодаря своей эффективности и малому энергопотреблению системы адиабатического охлаждения наилучшим образом подходят для организации круглогодичного фрикулинга в ЦОДе. Нужно только правильно выбрать тип системы и параметры ее работы.

Развитие индустрии производства ИТ-оборудования открывает новые возможности для организации системы охлаждения ЦОДа. Если буквально несколько лет назад мы и представить себе не могли систему охлаждения без компрессорной части или фреонового контура, то сегодня использование таких систем становится не просто возможным, а зачастую наиболее целесообразным. Температура в машинных залах ЦОДов, рекомендуемая для работы ИТ-оборудования, с каждым годом повышается, а значит, на все большей территории можно устанавливать в дата-центрах системы охлаждения с круглогодичным фрикулингом*.

Попробуем разобраться, что необходимо для реализации подобной системы.

Что говорит теория…

По сути, любая система охлаждения не холод создает, а переносит тепло от более нагретой среды к менее нагретой. Привычные системы охлаждения с кондиционерами и чиллерами переносят тепло от ИТ-оборудования из машинного зала на улицу, чтобы передать его уличному воздуху.

Процессы переноса тепла описываются законом Фурье:

$$\vec{q} = -\lambda \operatorname{grad} T, \text{ где}$$

$\vec{q}$ – вектор плотности теплового потока,

λ – коэффициент теплопроводности (удельная теплопроводность),

T – температура.

Минус в правой части показывает, что тепловой поток направлен противоположно вектору T (т.е. в сторону скорейшего убывания температуры).

Получается, что для передачи тепла из машинного зала на улицу необходимо, чтобы температура воздуха на улице была хотя бы на 1°C ниже, чем в машинном зале. На самом деле разница должна быть несколько больше, чем 1°C, поскольку в любой системе всегда присутствуют потери, которые зависят от ее организации и используемого оборудования и влияние которых по приблизительным оценкам эквивалентно 3°C. Чем больше разность температур между машинным залом и улицей, тем интенсивнее проходит процесс теплопередачи, иными словами, тем меньше «железа» и энергии нужно, чтобы охладить машинный зал.

Таким образом, чтобы создать максимально эффективную систему с минимальной стоимостью, необходимо увеличить разность температур между машинным залом и улицей. Для этого нужно повысить температуру в машинном зале или снизить максимальную для региона строительства ЦОДа температуру воздуха, поступающего с улицы, а лучше и то и другое.

С увеличением температуры в машинном зале все более или менее понятно, и индустрия движется в этом направлении, но что делать с максимальной температурой воздуха, поступающего с улицы?

Снизить температуру уличного воздуха можно с помощью систем адиабатического охлаждения. Такие системы подразумевают охлаждение воздуха за счет испарения воды.

Системы адиабатического охлаждения позволяют снизить температуру поступающего воздуха на 3–12°C в зависимости от организации системы, региона и способа испарения воды и, по сути, являются панацеей для регионов с сухим и жарким климатом.

Реализовать систему адиабатического охлаждения можно разными способами, из которых сегодня наиболее распространены два:

1. На основе PAD-панелей (матов) из специального пористого материала. Материал обильно смачивается водой, и воздух, проходя через него, насыщается влагой. При этом температура воздуха снижается.

* А. Эрлих. Круглогодичный фрикулинг в России, или Готовых рецептов нет. «ИКС» № 4'2019, с. 28.

2. При помощи форсунок, которые распыляют воду. Возможны два варианта:

- вода распыляется в воздух, при этом только часть воды испаряется, насыщая воздух и снижая его температуру, а остальное выпадает в осадок или уносится боковым ветром;
- вода распыляется на поверхность и испаряется с поверхности, снижая температуру воздуха.

Эффективность системы адиабатического охлаждения зависит от того, насколько удается охладить воздух за счет испарения воды, и ее можно рассчитать по формуле:

$$\text{Эффективность [\%]} = \frac{(T_1 - T_2)}{(T_1 - T_{\text{м.т.}})}, \text{ где}$$

T_1 – температура воздуха до адиабатического охладителя,

T_2 – температура воздуха после адиабатического охладителя,

$T_{\text{м.т.}}$ – уличная температура воздуха по мокрому термометру.

Эффективность системы адиабатического охлаждения оказывает решающее влияние на производительность теплообменного агрегата, потому что он, в свою очередь, сконструирован как устройство с воздушным охлаждением с температурой воздуха, достигаемой после адиабатического охлаждения. Эта температура одновременно является и температурой переключения на влажный режим.

...и о чем свидетельствует практика

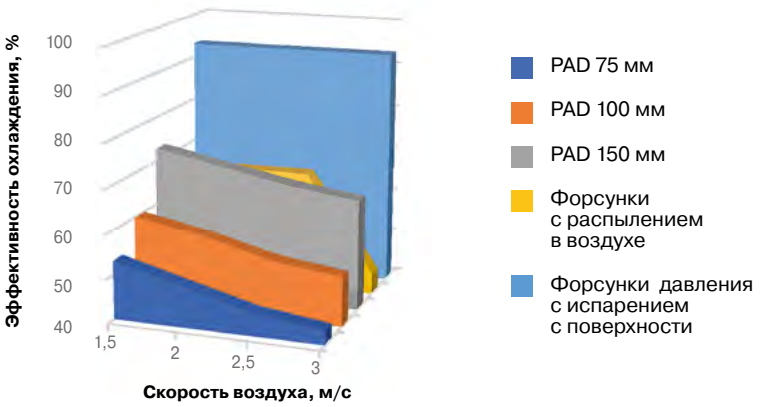
К сожалению, для агрегатов на основе адиабатического охлаждения в настоящее время нет ни единых процедур тестирования, ни сертификатов независимых организаций, подтверждающих их производительность. Поэтому коллегами из Германии было проведено исследование продукции более 10 производителей систем адиабатического охлаждения.

В ходе исследования изучалось влияние на эффективность адиабатического охлаждения следующих факторов:

- скорости движения охлаждаемого воздуха;
- сопротивления по воздуху (потери давления со стороны воздуха);
- расхода воды на орошение;
- температуры воды, используемой для орошения.

Исследование проводилось при температуре воздуха по сухому термометру 35°С, по мокрому термометру 22°С и нормальном атмосферном давлении.

Максимальную эффективность в исследовании продемонстрировали системы адиабатического охлаждения с использованием форсунок (рис. 1). При этом испарительное охлаждение с



▲ Рис. 1. Эффективность охлаждения в зависимости от скорости воздуха для различных адиабатических систем

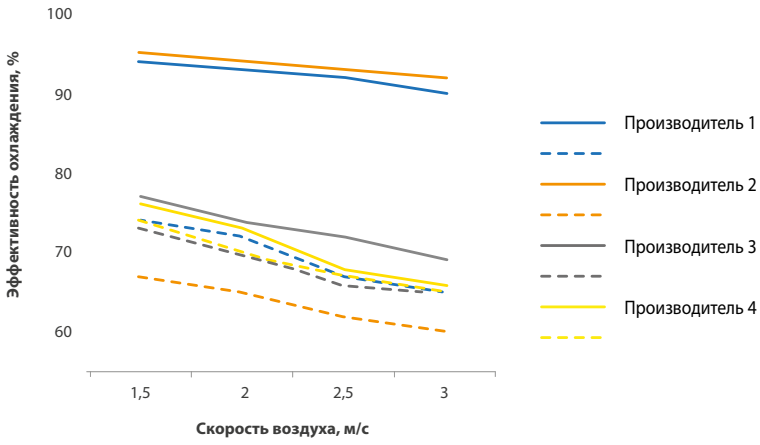
поверхности оказалось самым эффективным и мало зависящим от скорости движения воздуха. При распылении воды в воздух эффективность ниже, при скорости воздуха до 2,5 м/с она остается практически неизменной, а при дальнейшем росте скорости эффективность охлаждения заметно снижается.

Эффективность адиабатического охлаждения при использовании PAD-панелей зависит в первую очередь от их толщины: чем панель толще, тем она эффективнее. С увеличением скорости прохождения воздуха через PAD-панель эффективность охлаждения снижается.

Производители панелей, как правило, декларируют эффективность охлаждения при скорости воздуха в диапазоне 0,5–3 м/с. В процессе исследования выяснилось, что половина производителей сильно переоценивает эффективность своих панелей. На рис. 2 сплошными линиями показаны графики эффективности охлаждения, заявленной четырьмя разными производителями PAD для панелей толщиной 150 мм, а пунктиром – реальные графики эффективности, полученные экспериментально.

Заявляемые характеристики форсунок (пропускная способность, параметры купола раскрытия струи и др.) куда менее эфемерны и легко проверяются.

Рис. 2. Декларируемая и экспериментальная эффективность охлаждения в зависимости от скорости воздуха для PAD 150 мм ▼



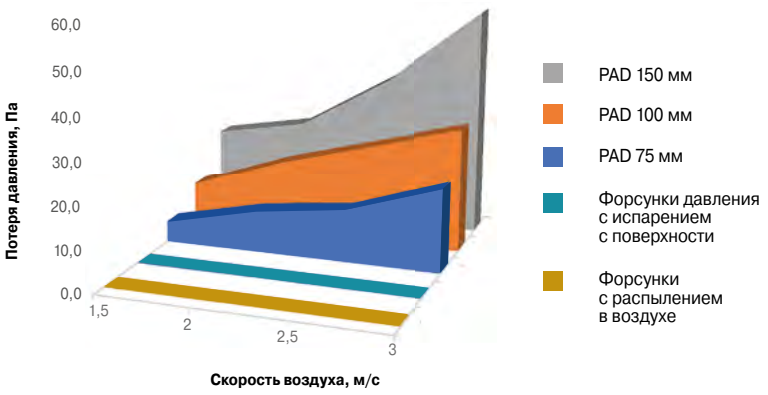


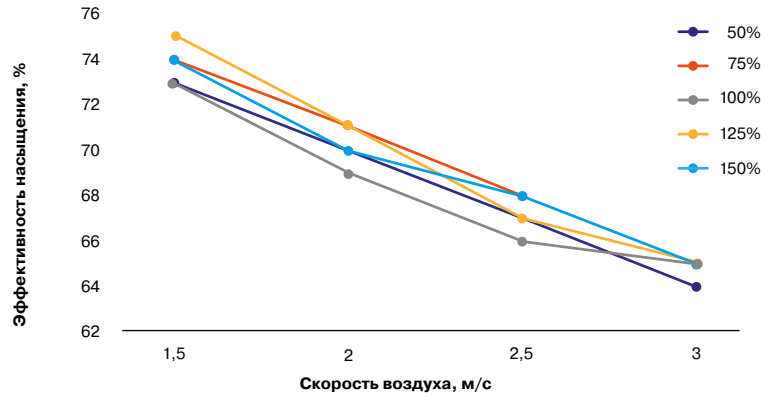
Рис. 3. ▲ Потери давления в системах адиабатического охлаждения в зависимости от скорости воздуха

Другой немаловажной характеристикой является сопротивление по воздуху той или иной системы адиабатического охлаждения. Эта характеристика не влияет напрямую на эффективность адиабатики, но оказывает огромное влияние на энергопотребление системы охлаждения в целом. Чем больше сопротивление потоку воздуха в адиабатической системе охлаждения, тем больше электроэнергии затратит вентилятор для его преодоления.

Системы с использованием форсунок не создают дополнительного сопротивления по воздуху, чего нельзя сказать о PAD-панелях (рис. 3). Как видно из графика, в системах с использованием PAD сопротивление потоку воздуха и связанный с ним рост энергопотребления тем больше, чем больше толщина и соответственно эффективность панели.

Поскольку система адиабатического охлаждения в большинстве случаев является неотъемлемой частью оборудования, бывает достаточно сложно ее демонтировать, скажем, на зимний период. В случае форсуночного орошения в этом нет необходимости. Если же вы отдали предпочтение PAD, готовьтесь к трудностям. Даже если производителем предусмотрена возможность снять панели, вам понадобится квалифицированный и физически сильный персонал, который сможет снять PAD-панели на зиму и установить их снова на лето. В противном случае система с PAD-панелями, работая лишь несколько часов в году, будет требовать дополнительного электроснабжения постоянно, создавая сопротивление потоку воздуха, которое вентиляторам необходимо будет преодолевать.

Рис. 4. Эффективность насыщения в зависимости от скорости воздуха при разном расходе воды, используемой для орошения ▼



При изменении расхода воды в диапазоне 50–150% от номинальных 100%, рекомендуемых производителями адиабатических систем охлаждения PAD, эффективность насыщения от скорости воздуха зависит незначительно (рис. 4).

В системах с использованием форсунок при изменении расхода воды эффективность насыщения остается также почти неизменной. Но при повышении расхода воды свыше 100% увеличивается объем дренажа.

Изменение температуры распыляемой воды эффективность насыщения меняет незначительно (см. таблицу). Настолько незначительно, что совершенно не оправдывает затрат на получение охлажденной воды для орошения.

Температура воды, ˚С	Эффективность насыщения, %	Изменение эффективности насыщения, %
36	66	-2,94
30	66	-2,94
20	68	0,00
14	69	1,47
7	70	2,94

▲ Эффективность насыщения в зависимости от температуры распыляемой воды

Итак, в ходе исследования было установлено, что наиболее эффективной является форсуночная система испарительного адиабатического охлаждения. Эта система не создает дополнительного сопротивления потоку воздуха, а значит, не требует дополнительной электроэнергии. Поэтому она оптимальна для обеспечения круглогодичного фрикулинга в ЦОДе.

Наибольшее влияние на системы испарительного адиабатического охлаждения оказывает скорость воздуха: чем она меньше, тем эффективнее система. Температура используемой воды почти не влияет на эффективность охлаждения, а расход воды в первую очередь влияет на объем дренажа, но мало сказывается на эффективности охлаждения.

Результаты исследования справедливы при применении адиабатического охлаждения в любом из компонентов климатической системы: чиллерах, конденсаторах, драйкулерах, системах вентиляции и т.д. ИКС

Тренды развития современных СКС

За последние десятилетия ИТ-отрасль изменилась столь разительно, что успевшие стать классическими принципы построения структурированных кабельных систем потребовалось модернизировать, причем как на системном уровне, так и на уровне элементной базы.

Андрей Семенов, профессор, МТУСИ

Кабельная техника, как известно, отличается консерватизмом. Постулаты построения СКС были сформулированы еще в конце 80-х гг. прошлого столетия, оформлены в виде набора стандартов в начале 90-х и за время существования этого технического направления доказали свою эффективность. Но три с лишним десятка лет, которые прошли с момента перевода внутриобъектовой информационной проводки на принципы структурированного каблирования, – огромный срок для динамично развивающейся ИТ-отрасли. Особенности функционирования более высоких уровней информационно-транспортной системы (ИТС), поддерживаемые приложения, скорости передачи данных и т.д. изменились так сильно, что потребовалась коррекция принципов построения СКС, которые к настоящему времени превратились в классические.

Цель всех рассматриваемых далее нововведений, часть которых уже стандартизована отраслевыми нормативными документами, а часть продолжает обсуждаться, – увеличение общей технико-экономической эффективности кабельной системы.

Отказ от одного типа горизонтального кабеля

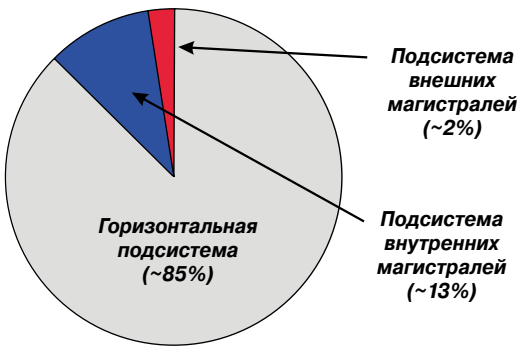
Известно, что на горизонтальную подсистему затрачивается примерно 85% всех ресурсов, необходимых для построения СКС (рис. 1). Высокие капитальные затраты на создание проводки, обусловленные избыточностью системы с точки зрения количества инсталлированных информационных розеток, в классических СКС частично компенсировались применением в горизонтальной подсистеме только одного типа кабеля. За счет этого, во-первых, снижалась отпускная цена компонентов вследствие роста объема их производства, а во-вторых, уменьшалось количество отходов, объем которых достаточно велик из-за индивидуального характера любого проекта, что делало в принципе невозможным применение претерминированных изделий заводского изготовления. Малость доли (не более 7%) стоимости СКС в общем объеме затрат на информационную систему на протяжении 10–15-летнего срока ее службы делала такой подход допустимым.

Сегодня ситуация изменилась. С одной стороны, резко, в разы выросли цены на медь и нефть – основные сырьевые материалы для изготовления горизонтального кабеля, являющегося главной статьей затрат на горизонтальную подсистему, а с другой – благодаря достижениям микроэлектроники существенно снизилась стоимость активного сетевого оборудования.

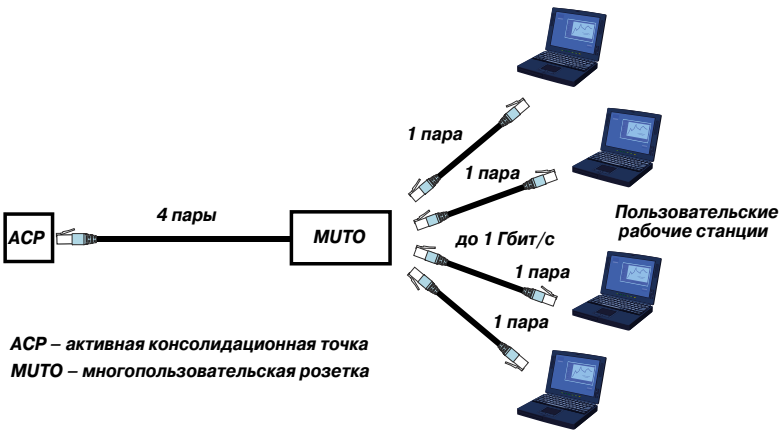
Восстановить экономическую привлекательность СКС можно только изменением базовых принципов построения, в первую очередь, ее горизонтальной подсистемы. Здесь возможны решения компонентного и системного плана. В части компонентов наибольший эффект дает обращение к однопарному кабелю при условии сохранения технологии Ethernet в качестве средства транспорта данных.

Переход на однопарные изделия имеет следующие преимущества:

- существенное (по оценкам, примерно в 2,5 раза) уменьшение затрат на создание горизонтальной подсистемы и сопутствующей инфраструктуры информационной проводки за счет



◀ Рис. 1. Типовая структура затрат на создание крупной СКС



▲ **Рис. 2. Схема подключения рабочих станций ЛВС к многопользовательской информационной розетке**

уменьшения количества пар и средней протяженности линии;

- сохранение привычного для пользователя уровня информационной поддержки благодаря обеспечению скорости передачи данных вплоть до 1 Гбит/с;
- отсутствие необходимости выполнения масштабных НИОКР: техника однопарного Ethernet прямо заимствуется из промышленных систем.

Однако полный отказ от четырехпарной техники невозможен и нецелесообразен по целому ряду причин:

- потребность в передаче 10-гигабитных потоков велика даже в офисных ИТС;
- мощность дистанционного питания в принципе не может быть выше 50 Вт, что недостаточно для большой группы терминальных устройств;
- в открытых офисах получила широкое распространение простая и удобная зонная схема построения СКС на основе активной консолидационной точки (Active Consolidation Point, ACP) и многопользовательской розетки в сочетании с применением принципа cable sharing и технологии port trunking (рис. 2).

Рост значения экранированной техники и техники высоких категорий

Действующими и перспективными стандартами СКС допускается реализация ключевой

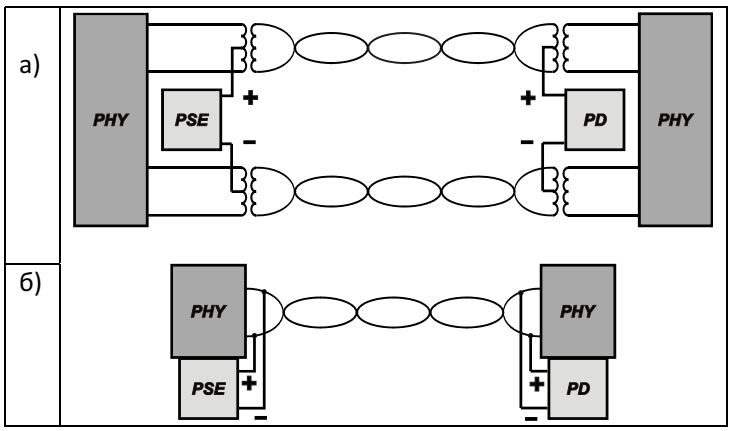


Рис. 3. Варианты организации дистанционного питания по кабельным трактам СКС: а) двухпарный тракт PoE; б) PoDL по однопарному тракту ▼

для информационной проводки горизонтальной подсистемы как на электропроводной, так и на волоконно-оптической элементной базе без конкретизации условий выбора одной из них. Четверть века назад ожидалось, что волоконно-оптическая техника вытеснит электропроводную, но этого не произошло, несмотря на широкое распространение IP-видеотелефонии, которая считалась драйвером развития оптоволокна. Сохранению позиций электропроводной техники способствовало создание элементной базы категорий 5e и выше, обеспечивающей передачу информационных потоков со скоростью 1 Гбит/с и более. Поскольку среднестатистический пользователь не в состоянии полноценно воспринимать информацию, поступающую к нему со скоростью свыше 50 Мбит/с, таких скоростей для работы офисных ЛВС достаточно. Еще одним фактором, продляющим жизнь электропроводных линий, стала возможность дистанционного питания через них маломощных терминальных приборов по технологиям PoE (четырехпарные тракты) и PoDL (однопарная техника) (рис. 3). Различия в аббревиатурах для обозначения технологий объясняются различием в схемах доставки тока питания от источника (Power Sourcing Equipment, PSE) до потребителя (Powered Device, PD): в случае PoE используются фантомные цепи, а в случае PoDL — обычная пара в комбинации с высокоомным для переменного тока источником.

Востребованность техники PoE и PoDL главным образом и побуждает специалистов создавать СКС на основе кабелей более высокой категории. Сказывается необходимость применения в горизонтальных кабелях категории 6 и выше проводов витых пар с жилами увеличенного диаметра, которые намного лучше подходят для обеспечения работоспособности терминальных устройств высокой мощности. Количество таких потребителей ресурсов СКС растет, и основную их массу составляют системы управляемого светодиодного освещения, а также 2,5- и 5-гигагерцовые точки радиодоступа Wi-Fi, которые из-за ограниченного радиуса действия отличаются повышенной плотностью установки даже в открытых офисах.

Еще один тренд развития СКС – рост популярности разных вариантов экранированной техники, обусловленный расширением рабочего частотного диапазона. С точки зрения межкабельной переходной помехи линейные изделия, которые являются основным их источником, при скорости передачи 10 Гбит/с даже в варианте F/UTP существенно лучше, чем U/UTP-решения, противостоят как влиянию соседних кабелей, к которым подключены такие же интерфейсы, так

и влиянию кабелей, по которым работают относительно узкополосные гигабитные интерфейсы. Последнее важно потому, что пропускная способность симметричного кабельного тракта определяется преимущественно его параметрами в низкочастотной части спектра (рис. 4).

Определенное значение имеет также меньший рост затухания из-за нагрева при высоких мощностях дистанционного питания, который отмечается на кабельных трактах большой длины, в случае использования экранированных кабелей. Дело в том, что экранирующие покрытия даже в варианте тонкой металлизированной фольги становятся эффективным радиатором, который отводит тепло, выделяемое жилами при прохождении тока питания.

Системные изменения на уровне горизонтальной подсистемы

Значимое снижение затрат на построение горизонтальной подсистемы СКС обеспечивается переходом на зонную схему построения проводки с использованием активной консолидационной точки (рис. 5). Применение такой топологии дает следующие выгоды:

- примерно вдвое уменьшает расход горизонтального кабеля (наиболее затратной части проводки);
- позволяет сохранить привычный для проектировщиков, инсталляторов и служб эксплуатации 90-метровый предел протяженности стационарной части СКС, реализуемой в данном случае по неоднородной схеме (см. таблицу на с. 62);
- заметно разгружает технические помещения от активного сетевого оборудования уровня рабочей группы за счет выноса последнего в АСР.

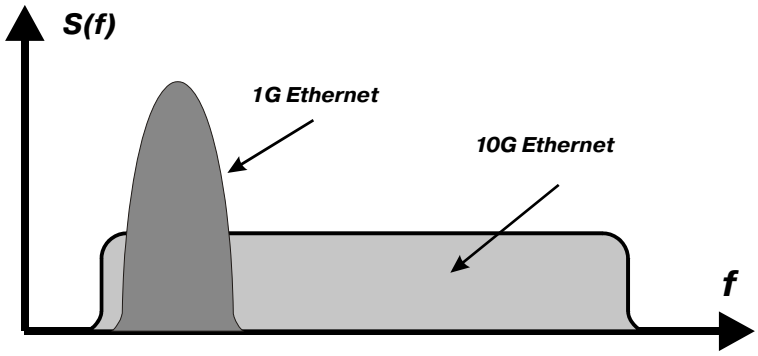


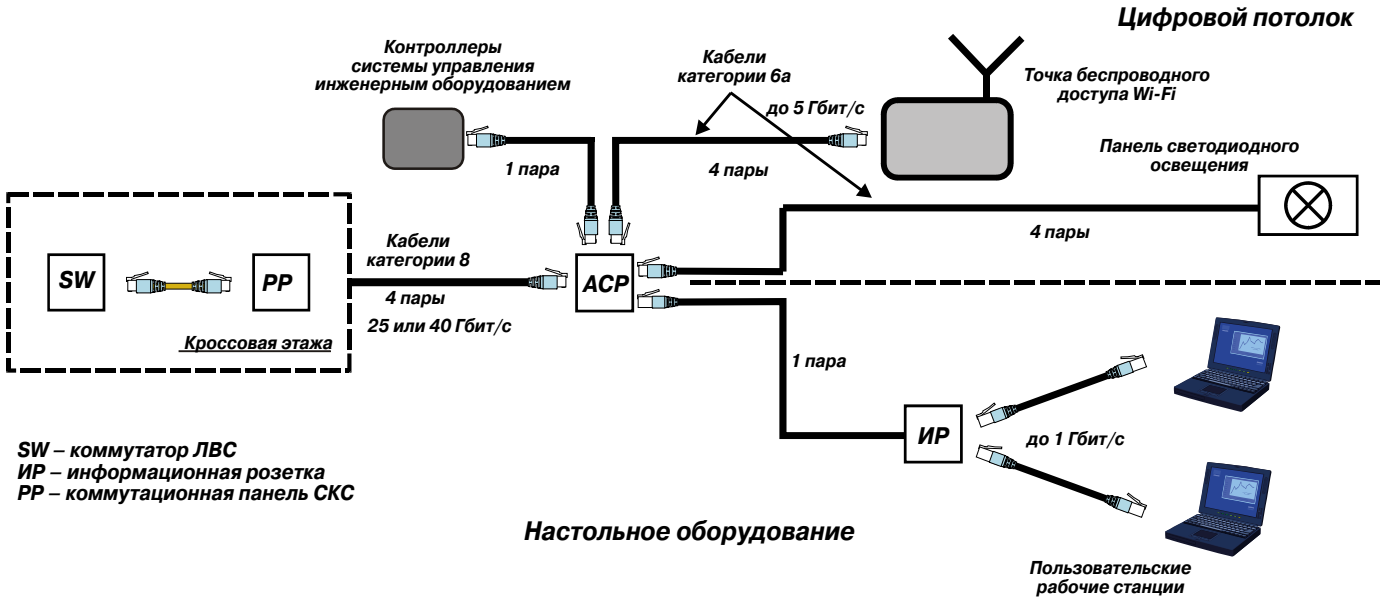
Рис. 4.▲ Взаимодействие спектров линейных сигналов интерфейсов 1G Ethernet и 10G Ethernet

Техническая возможность применения такой структуры поддерживается полным переводом ЛВС на коммутирующие концентраторы, которые делают ненужным соблюдение правила четырех репитеров (оно было актуальным в сетях Ethernet с общей средой передачи. – *Прим. ред.*), и построением ИТС на единой технологической платформе коммутации и маршрутизации IP-трафика.

Необходимость подключения коммутатора АСР к 220-вольтовой сети дополнительно обеспечивает возможность полноценного питания терминального оборудования по технологиям PoE и PoDL.

В современной ИТС, как правило, присутствует большое количество устройств верхней установки (точки радиодоступа Wi-Fi, камеры телевизионного наблюдения, управляемые панели светодиодного освещения и т.п.), которые образуют так называемый цифровой потолок. Появление цифрового потолка с его многочисленными стационарными устройствами, к которым не требуется постоянного доступа пользователей, заметно расширяет поле применения новых конфигураций горизонтальных трактов. Речь идет о трактах типа direct connection и end-to-end (рис. 6).

Рис. 5. Структура нижнего уровня ИТС в случае применения активной консолидационной точки ▼



Предельная протяженность трактов при различных вариантах реализации неоднородной электропроводной горизонтальной проводки в случае применения активной консолидационной точки ▶

Групповая часть		Индивидуальная часть		Общая длина линии, м
Скорость, Гбит/с	Длина линии, м	Кабели F/UTP	Кабели U/UTP	
40	30	40	15	70/45
25	50	40	15	90/65

Волоконно-оптическая подсистема

Основной драйвер развития волоконно-оптической техники СКС – ЦОДы, которые становятся опорными элементами информационной инфраструктуры и количество которых в мире и в России быстро растет. При этом потребность в сокращении времени реакции на поступающий пользовательский запрос заставляет, в частности, использовать высокоскоростные каналы внутренней связи. С другой стороны, у СКС, разворачиваемой в машинном зале ЦОДа, нет «белковых» потребителей ресурсов, что снимает ограничения на быстродействие аппаратуры и канала связи как ее части, обычно присутствующие в системах «человек – машина».

Необходимость организации в ЦОДе высокоскоростного информационного обмена (в текущем году количество вновь поставляемых 100-гигабитных сетевых интерфейсов превысило аналогичный показатель для 40-гигабитных) с учетом ограниченного быстродействия современной микроэлектроники вынуждает применять схему параллельной передачи. Она реализуется в вариантах пространственного или спектрального мультиплексирования либо их комбинации, что на примере 100-гигабитной системы демонстрирует рис. 7.

Рис. 6.
Варианты построения трактов горизонтальной подсистемы ▼

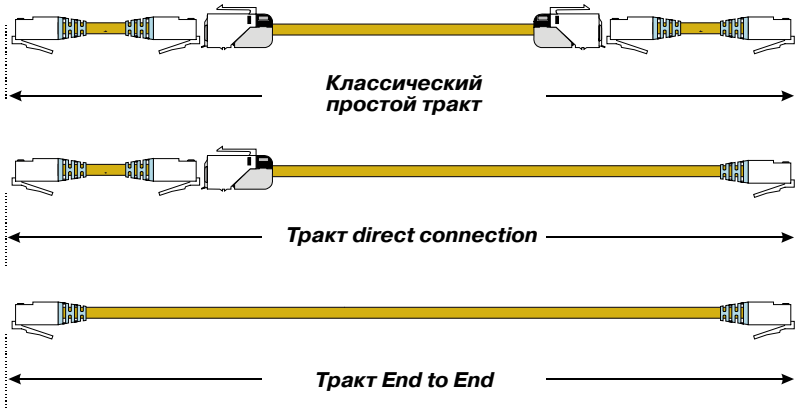
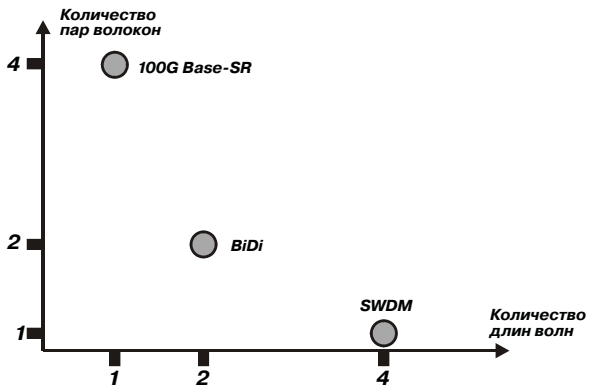


Рис. 7.
Спектрально-волоконная диаграмма вариантов реализации параллельной передачи ▶



В процессе разработки первого американского национального нормативного документа на СКС для ЦОДов (соответствующего раздела стандарта ANSI/TIA-942) в качестве группового соединителя был принят MPO/MTP, поддерживающий в однорядном варианте коммутацию одновременно 12 волокон. Простота перехода на более высокие скорости передачи и правильная раскладка волокон в кабельных трактах на основе этого соединителя обеспечиваются применением модульно-кассетных решений и так называемой универсальной полярности (разработки компаний Corning, Leviton, Commscope и Reichle De-Massari).

Основная сложность применения соединителей MPO/MTP состоит в следующем. Со схемотехнической точки зрения количество каналов параллельной передачи целесообразно выбирать равным целочисленной степени 2. Однако 12-волоконный MPO/MTP при его использовании в составе линий класса Base8 (восемь активных волокон) не вполне подходит на эту роль. Возможный выход – модернизация MPO (результатом которой стал популярный 16-волоконный разъем MPO16 в однорядном исполнении) или создание специализированного разъема. Работы в этом направлении привели к созданию довольно удачных соединителей CN (японской компанией Senko) и MDC (американской компанией US Conec).

Соединители CN и MDC имеют следующие особенности:

- реализация на наконечниках диаметром 1,25 мм;
- возможность эксплуатации в виде как дуплексной моноблочной вилки, так и сдвоенной или счетверенной сборки;
- полное соответствие дуплексному разъему LC по площади миделя в восьмиканальном варианте, т.е. потенциальная взаимозаменяемость по посадочным местам (важно с точки зрения возможности увеличения скорости передачи канала).

Все это позволяет считать данные изделия родоначальниками нового класса сверхкомпактных оптических разъемов.

Отказ от жесткого задания предельной протяженности кабельных трактов

Одним из канонов СКС была фиксация предельной протяженности тракта той или иной подсистемы. Таковыми значениями являлись 100 м для горизонтальной подсистемы, 300 (500) и 2000 м для магистральных подсистем. В настоящее время от этого постулата все чаще отказываются в пользу подхода «под приложение» с учетом области применения. Главная причина – перевод ИТС на единую платформу Ethernet.

Например, в ЦОДах на расстояниях 28–32 м могут быть задействованы медножильные кабели категории 8, а в случае волоконно-оптической элементной базы длина прокладываемых линий может составлять 70, 100 и 150 м даже для скоростей 100 Гбит/с и более. В офисах тракты, обеспечивающие подключение точки радиодоступа Wi-Fi к ИТС со скоростями 2,5 и 5 Гбит/с, реализуются на медножильной элементной базе категорий 5e и 6 при условии дополнительной пересертификации и могут иметь длину 50 и 75 м. Для систем видеонаблюдения существуют предложения «длинного Ethernet», позволяющие без применения репитеров добиться дальности связи свыше 200 м на скорости 100 Мбит/с по витой паре с характеристиками 5e по переходной помехе.

Для того чтобы сделать текущее администрирование СКС более удобным, массово предлагаются тонкие коммутационные шнуры с жилами, диаметр которых уменьшен до калибра 28AWG. Незначительное, примерно на 5 м, уменьшение предельной протяженности тракта с лихвой окупается удобством чтения маркировки панелей. Возможность такого решения обосновывается статистикой реализованных проектов, согласно которой свыше 95% стационарных линий имеют длину не более 75 м.

■■■

Структурированные кабельные системы – пассивное оборудование информационных систем – продолжают развиваться как на уровне элементной базы, так и на системном уровне.

Ряд объективных технических причин способствует все более широкому применению экранированной техники. В ближайшие годы возможен массовый перевод наиболее ресурсоемкой горизонтальной подсистемы СКС с четырехпарного на однопарное исполнение в сочетании с ее построением на основе двух подуровней, интегрируемых в единое целое активной консолидационной точкой. Однако полный отказ от четырехпарного кабеля из витых пар невозможен.

В ЦОДах главной схемой организации волоконно-оптических трактов становятся Base8 и ее производные.

«Универсальные» ограничения предельной протяженности кабельного тракта как электропроводной, так и волоконно-оптической подсистем постепенно заменяются ограничениями, которые определяются приложениями. ИКС

Дорогу модульным!

В последнее время заметна тенденция применения в ЦОДах модульных ИБП – аппаратов, в которых требуемая мощность обеспечивается несколькими силовыми модулями относительно малой мощности, включенными параллельно и интегрированными в один конструктив, чаще всего в 19” стойку.

Современный ЦОД невозможно представить без источников бесперебойного питания, защищающих IT-оборудование и инженерные системы от некачественного электропитания. До недавних пор в ЦОДах устанавливали преимущественно ИБП моноблочного исполнения, в которых вся выходная мощность предоставляется одним силовым блоком. Появление на рынке модульных ИБП сопровождалось и сопровождается мнениями «за» и «против» модульных решений.

Еще лет пять назад в модульных ИБП применялись силовые блоки мощностью 10–30 кВА, и разумное ограничение числа подключаемых силовых модулей (10–20 шт.) не позволяло создавать модульные системы мощнее 200–300 кВА. Поэтому считалось, что модульные ИБП подходят только для малых и средних ЦОДов, для крупных же объектов пригодны исключительно моноблочные решения. При этом эксперты, обсуждая перспективу роста мощности силовых модулей, прогнозировали пропорциональное увеличение их веса, которое исключит возможность оперативной замены вышедшего из строя модуля.

Модульные ИБП MR33, которые выпускает компания Kehua Tech, поначалу действительно имели силовые модули мощностью 25 кВА/25 кВт и весом 32 кг. Затем компания ввела в производство силовые модули 50 кВА/50 кВт весом 33 кг, что позволило наладить выпуск модульных ИБП серии MR33 в диапазоне мощностей от 25 до 600 кВА. В начале текущего года было запущено производство ИБП с модулями 80 кВА/80 кВт с максимальной мощностью в единичном конструктиве до 800 кВА/800 кВт. При этом силовой модуль 80 кВт имеет высокую удельную мощность и весит 41 кг, что еще допускает его замену в экстренной ситуации ручным способом без применения подъемных механизмов.

Следующим аргументом в пользу применения моноблочных решений именно в ЦОДах, по мнению экспертов, был недостаточно высокий КПД модульных ИБП. Это особенно проявлялось при малых нагрузках, имеющих место при изменяющемся суточном графике потребления и реализации различных схем резервирования. Пониженный КПД объясняется большим количеством работающих полупроводниковых элементов и работающих вентиляторов, неидеальной синхронизацией силовых модулей, обуславливающей наличие уравнительных токов между силовыми модулями и, соответственно, дополнительные потери.

Сегодня ситуация изменилась. Например, КПД ИБП Kehua серии MR33 500 кВА достигает 96% уже при 35%-ной нагрузке (рис. 1).

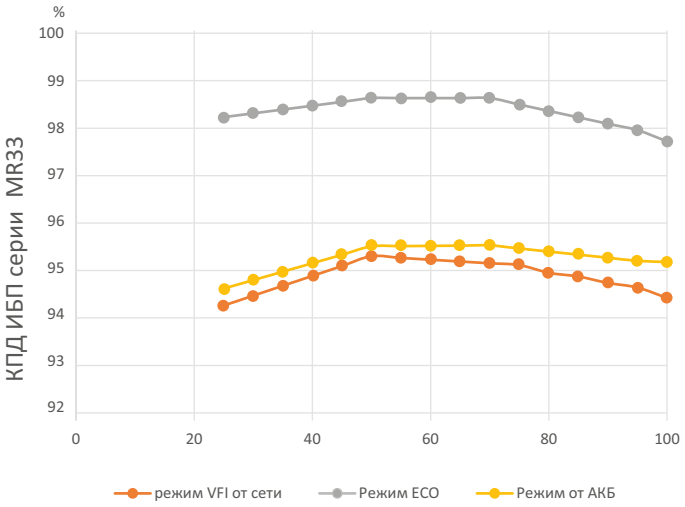


Рис. 1. Зависимость КПД от нагрузки для модульного ИБП MR33 500 кВА из 10 силовых модулей MR3350-J (50 кВА/50 кВт)

Высокий КПД MR33, не опускающийся в режиме двойного преобразования ниже 94% в диапазоне нагрузок от 20 до 100% – очень хороший показатель даже для моноблочных систем.

Повышение КПД модульных ИБП MR33 достигнуто за счет совершенствования схемотехники силовых модулей, алгоритмов их точной синхронизации, применения более эффективных вентиляторов, использования режима «спящих модулей» (рис. 2).

Рис. 2. Режим «Спящие модули»

В таком режиме ИБП постоянно отслеживает текущий уровень нагрузки относительно суммарной максимальной мощности установленных в ИБП силовых блоков. При уменьшении нагрузки ниже наперед установленного уровня ИБП выводит некоторые модули из работы, сохраняя их синхронизацию. За счет перераспределения нагрузки между оставшимися в работе силовыми

ИБП Kehua Tech
KR 33 300–1200 кВА

ИБП Kehua Tech
MR 33 25– 800 кВА

модулями происходит повышение их КПД и КПД ИБП в целом.

Вторым положительным эффектом такого режима работы является увеличение срока службы вентиляторов охлаждения – в спящих модулях они не работают. Ротация спящих и работающих модулей позволяет обеспечивать равномерную наработку всех компонентов ИБП на отказ (MTBF – среднее время наработки на отказ, или, в дословном переводе, среднее время между отказами).

А более низкий показатель MTBF, обычно свойственный модульным ИБП, является еще одним фактором, ограничивающим, по мнению экспертов, их применение в ЦОДах.

MTBF – величина расчетная и зависит, во-первых, от вероятностей отказов компонентов и разъемных соединений, входящих в электронное устройство, и во-вторых, от количества этих компонентов.

Моноблочные ИБП имеют более высокий MTBF, чем модульные. Причина проста: в модульных ИБП больше электронных компонентов и разъемных соединений, каждый из которых рассматривается как потенциальная точка отказа. Соответственно, теоретически возможность отказа здесь выше. Но модульные ИБП практически не применяются без резервирования силовых блоков. Резервные силовые блоки повышают MTBF. Кроме того, для ИБП в ЦОДе критичен не столько сам отказ, сколько то, как долго ИБП будет оставаться в нерабочем состоянии.

И здесь преимущество уже на стороне модульных ИБП: они отличаются низким значением MTTR (среднее время на замену), потому что и силовые модули, и байпас можно оперативно заменить без перерыва в электроснабжении нагрузки («горячая» замена модулей). Kehua MR33 не требует отключения и/или перевода ИБП на байпас для замены силового модуля, модуля байпаса и плат управления.

Подводя итог сказанному, можно сделать вывод: сегодня при построении систем электроснабжения ЦОДов, в том числе мощных, не существует принципиальных ограничений для использования ИБП модульной архитектуры. Выбор между блочным и модульным решениями стал менее очевидным, однако эксперты Kehua Tech отмечают несколько сценариев, когда применение модульных ИБП выглядит наиболее целесообразным:

- мощность ЦОДа планируется наращивать постепенно, и срок выхода на проектную мощность не определен на начальном этапе. Чем больше будут различаться стартовая и итоговая мощность ЦОДа, тем больше будет ощущаться финансовый эффект такого решения;
- текущая потребляемая мощность машинных залов ЦОДа может меняться в широких пределах в ходе эксплуатации;
- при создании или реконструкции ЦОДа могут возникнуть сложности с доставкой туда тяжелого моноблочного оборудования;
- ЦОД находится на значительном удалении от сервисного центра, когда максимально низкий MTTR можно обеспечить «горячей» заменой блоков эксплуатирующим персоналом.

Компания Kehua Tech, имея в портфеле выпускаемой продукции модульные и моноблочные ИБП широкого мощностного диапазона, всегда готова предложить оптимальное решение для надежного электроснабжения конкретного ЦОДа.

Дороги PaaS

Николай Носов

Облачные платформы позволяют разработчикам использовать самые современные решения на самых мощных компьютерах. Облачный провайдер откроет все пути, останется только проехать по выбранной дороге, дороге PaaS.

Привлекательна в платформенных сервисах и простота использования: если сервис подошел, его легко масштабировать, если нет – так же легко отказаться. Не надо думать о «железе», администрировании и поддержке ПО. Ничто не отвлекает от главной цели – создания продукта.

Больше PaaS – хороших и разных

Процессы цифровой трансформации переводят компании самых разных отраслей на цифровые рельсы, пандемия и связанные с ней ограничения служат катализатором таких изменений. Увеличивается число бизнес-задач, увеличивается и число платформенных сервисов, помогающих в их решении.

«Развитие PaaS – безусловно, самое интересное из того, что происходит сегодня в облаках. Текущему году мы обязаны тем, что PaaS-сервисы были массово замечены заказчиками и мгновенно стали востребованы. Именно за PaaS-сервисами компании пошли в облака, и активизировались те, кому были не очень интересны обычные сервисы IaaS, в первую очередь команды разработки крупных компаний. Сейчас наличие консистентной линейки PaaS-сервисов дифференцирует облачных провайдеров: одни могут что-либо предложить заказчикам, другие, увы, нет», – считает директор департамента ИТ-решений Huawei Артур Пярн.

Все дороги ведут к одной цели – решению бизнес-задач компании. Но популярность маршрутов разная. Некоторые хорошо обкатаны, подобны автомагистралям, по которым несется множество клиентов. Таково, например, предоставление базы данных из облака (dbPaaS), освобождающее разработчика от рутинной работы по администрированию. Для загрузки данных в новую базу и выполнения запросов к ним требуются считанные минуты (→ см. с. 71). Другие – почти тропинки, только наметки пути, по которым идут самые отважные первопроходцы. Так, направление GeoAI появилось совсем недавно и еще ждет поддержки со стороны облачных провайдеров.

Основная причина роста интереса к сервисам PaaS – обострение конкуренции на рынке и, как следствие, потребность в кастомизированных решениях, как раз и дающих бизнесу конкурентные преимущества. Сказывается увеличение проникновения облачных услуг, востребованность которых резко выросла в период пандемии COVID-19, и повышение доверия к облакам со стороны крупного бизнеса. В условиях экономического кризиса компании с осторожностью делают капитальные вложения, оптимизируя затраты на ИТ-инфраструктуру за счет использования облачных вычислений. Ведущие облачные провайдеры стали уделять больше внимания платформенным сервисам. На рынок выходят серьезные игроки, ранее облаками не занимавшиеся. Например, на сервисы PaaS приходится уже почти половина выручки «Яндекса» (→ см. с. 69).

Свою роль играет и государство. Сильное влияние на облачный рынок оказали нацпрограмма «Цифровая экономика РФ» и действия регуляторов (поправки в законодательство о защите персональных данных, политика импортозамещения, блокировки Роскомнадзора), которые заставляют задуматься о смене зарубежных «дорог» на отечественные. Именно так поступила, скажем, компания «Ашан Ритейл Россия» (→ см. с. 72).

> К числу наиболее популярных в публичном облаке сервисов PaaS отнес бы сервисы баз данных, Kubernetes и облачное (объектное) хранилище. Многие компании начали использовать в разработке контейнеры, и Kubernetes как инструмент стал более зрелым, избавился от «детских болезней». Добавим сюда различные программные средства для автоматизации DevOps-процессов. Разработка становится более быстрой и легкой, значит, клиент быстрее получит запланированные к релизу «фичи»».

Александр Тугов, директор по развитию услуг, Selectel

Тенденции развития PaaS

Постепенно размываются границы между классическими PaaS- и IaaS-сервисами. И те и другие можно рассматривать как разные способы предоставления платформенных сервисов для приложений, ориентированных на облако (cloud native). Облако развивается как конструктор, в котором сервисы PaaS и IaaS взаимосвязаны, и когда появляется новый

> Взрывной рост популярности носимых устройств и голосовых помощников послужит в ближайшие годы драйвером развития платформенных сервисов для быстрого создания IoT-решений, а также продуктов для машинного обучения и анализа естественного языка на базе искусственного интеллекта.

Дмитрий Лазаренко, директор по продукту, Mail.ru Cloud Solutions

Александр Липкин, директор департамента по технологическому развитию и поддержке ключевых заказчиков в России, Microsoft

Отдельно хотелось бы выделить вектор развития cloud native-приложений, построенных на микросервисной архитектуре с использованием контейнеров Kubernetes и бессерверных вычислений в облаке. В этом контексте особенно актуально использование в организации принципов и практик, применяемых сообществами разработчиков ПО с открытым кодом. Также стоит отметить тенденцию к переносу разработки ИТ-решений из централизованных ИТ-департаментов в бизнес-подразделения, что способствует активному развитию low code-платформ.

сервис, необходимо не просто презентовать его рынку, но и обеспечить взаимодействие с существующими. Поэтому в ближайшие годы наряду с выводом новых сервисов будет происходить все более тесная их интеграция внутри платформ.

На российском рынке также заметна тенденция строительства компаниями цифровых отраслевых продуктов на базе внешних платформ. В качестве фундамента для построения большинства современных продуктов используются контейнеры Kubernetes.

С технической точки зрения сегмент PaaS будет стремиться к упрощению подключения и эксплуатации, а также к большему проникновению бессерверных технологий. «Уже сейчас мы видим спрос на «инфраструктуру по клику», для которой компании не нужно покупать и настраивать оборудование. Дальше спрос будет только возрастать», – отмечает директор по продукту Mail.ru Cloud Solutions Дмитрий Лазаренко.

Среди других тенденций, выделяемых экспертами, – применение PaaS для разработки систем искусственного интеллекта, широкое использование средств аналитики в прикладных и бизнес-системах, а также в экосистемах интернета вещей.

Модели PaaS-партнерства

В российских условиях экосистемы PaaS в основном складываются вокруг якорного клиента и его партнеров. Якорным клиентом, как правило, выступает материнская компания облачного провайдера. Крупный бизнес либо создает свое облачное подразделение, которое начинает работу и с внешними заказчиками, либо покупает успешного облачного провайдера, интегрируя его в свои структуры. Примерами первого подхода служат SberCloud, дочка Сбербанка, и Mail.ru Cloud Solutions, примерами второго – купленные «Ростелекомом» компании «Тионикс» и DataLine. Основная модель партнерства – материнская компания отвечает за заказы (нагрузку на сервисы облачного провайдера), провайдер обеспечивает их выполнение в рамках SLA, попутно предоставляя сервисы сторонним заказчикам.

Все чаще проявляемое заказчиками желание получить мультиоблачные PaaS-решения не всегда находит отклик у провайдеров. Так, гиперскейлеры неохотно идут навстречу клиентам, пытаясь удержать их на своей платформе. Александр Ложечкин, руководитель архитектуры партнеров в регионе EMEA Amazon Web Services, подчеркивает ограничения мультиклаудного подхода:

- мультиклауд заставляет опираться на наименьший общий знаменатель нескольких платформ. В случае AWS, например, этот общий знаменатель в силу широкой функциональности платформы окажется мал, что не даст заказчику возможности воспользоваться всеми преимуществами облачных технологий;
- выбор мультиклауда заставит разработчиков говорить одновременно на нескольких языках, что сложно и сильно снижает производительность труда;
- облачный провайдер, как правило, предоставляет скидки при большом объеме потребляемых услуг, поэтому, распределяя нагрузку по нескольким поставщикам, компания лишается возможности получать эти скидки и в итоге больше теряет, чем приобретает.

Несмотря на приведенные доводы, и среди крупных игроков начали возникать взаимовыгодные альянсы с объединением решений разных облачных платформ, например, Microsoft Azure и Oracle Cloud.

Сотрудничество мировых лидеров и российских облачных провайдеров PaaS-сервисов в основном одностороннее – российские компании предлагают зарубежные сервисы из своего облака, зарабатывая на предоставлении услуг в соответствии с требованиями российских регуляторов (отчетные документы, оплата в рублях). Впрочем, появляются и более равноправные партнерства, например федерация кластеров Kubernetes в облаках AWS и Mail.ru Cloud Solutions, которую уже протестировала компания Bitrix24. В данном случае клиент платит каждому из провайдеров отдельно за использование мощностей. На маркетплейсе AWS услуга пока не появилась, так что взаимодействие идет только на техническом уровне.

Кому война – а кому мать родна

В числе драйверов развития облачного рынка игроки называют пандемию COVID-19, которая оказала неоднозначное влияние на рынок PaaS. Директор департамента по технологическому развитию и поддержке ключевых заказчиков компании Microsoft Александр Липкин отмечает: «Кроме очевидного роста спроса на сервисы для удаленной работы, мультифакторную аутентификацию и т.д., мы наблюдаем повышенный интерес к облачным платформам для обеспечения гибкости использования ИТ-ресурсов и сервисов, поскольку для многих компаний они являются возможностью оптимизировать расходы на ИТ-инфраструктуру».

Схожую тенденцию подмечает и Д. Лазаренко из MCS: «В пандемию мы увидели значительный рост спроса на Kubernetes, который объясняется востребованностью сервиса в сегменте электронной коммерции. В целом объем сегмента PaaS увеличился за время пандемии и продолжает активно увеличиваться, поскольку помогает компаниям быстрее и эффективнее справляться с повышающейся нагрузкой и передавать в зону ответственности провайдера те части ИТ-процессов, экспертиза в которых не критична для бизнеса».

По мнению операционного директора «Яндекс. Облако» Олега Ковернзева, все события на рынке облачных услуг немного померкли на фоне COVID-19 и перехода на удаленную работу. Хотя краткосрочные эффекты пандемии уже закончились, но многие решения, которые были приняты в компаниях, отменить уже нельзя. COVID-19 ускорил запуск некоторых проектов и изменил паттерны потребления людей и компаний.

Источник: iKS-Consulting

Среди основных факторов, сдерживающих развитие рынка PaaS, эксперты выделяют экономический спад, недостаток финансовых ресурсов и сокращение числа компаний-клиентов в условиях пандемии и экономического кризиса. Проблемой остается нехватка квалифицированных кадров, умеющих грамотно задействовать преимущества PaaS. В руководстве многих компаний отсутствует единое понимание процессов трансформации и важности использования облачных услуг. Тормозом является и неисполнение государством федерального бюджета по нацпроектам.

Несмотря на перечисленные трудности, развитие сегмента идет. Увеличивается число задач, стоящих перед бизнесом, растет и спрос на услуги PaaS. По оценкам iKS-Consulting, объем рынка PaaS в 2019 г. составил 5,1 млрд руб., в 2020-м он достигнет почти 6,1 млрд руб. и, увеличиваясь ежегодно на 20%, в 2024 г. вырастет до 11 млрд руб.

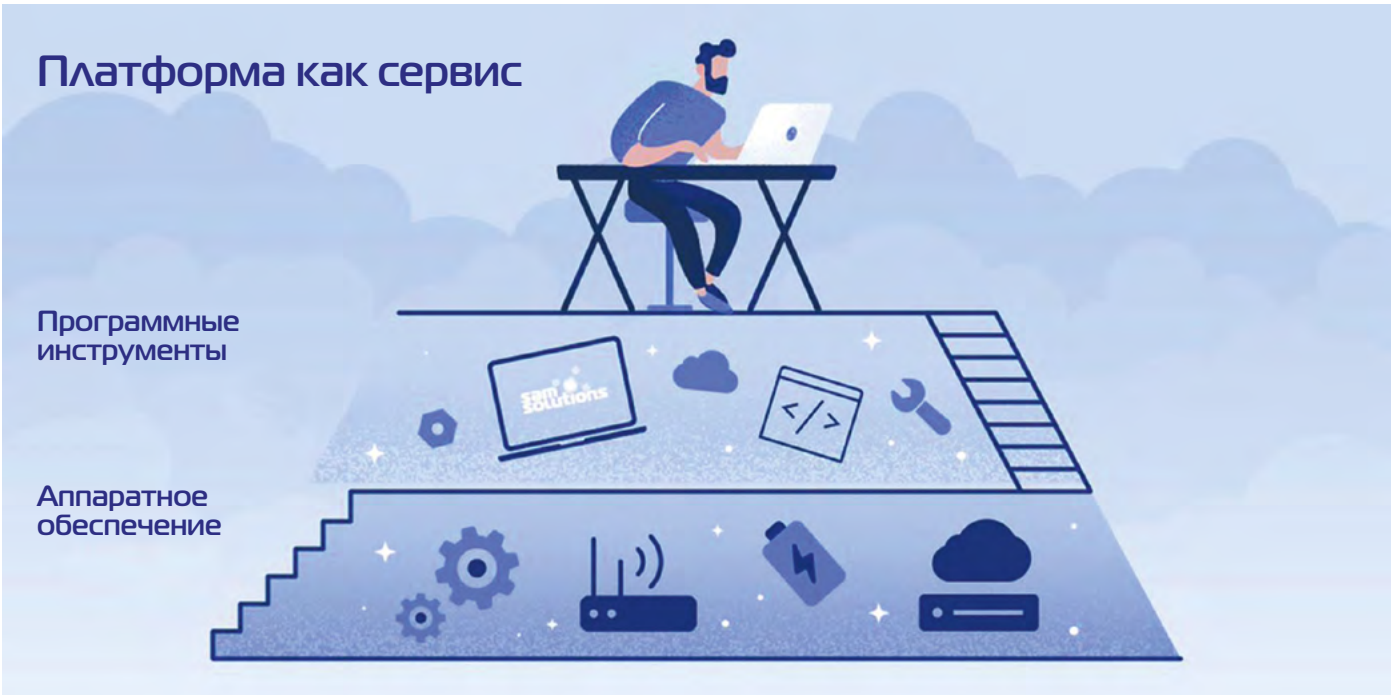
Обратного хода не будет

Краткосрочные эффекты пандемии закончились, но компании уже ощутили, что сервисы PaaS – надежный фундамент для построения бизнес-систем. Востребованность облачных платформ растет, и тенденция продолжится вне зависимости от ограничительных мер.

Цифровизация и пандемия

Весна выдалась очень насыщенной – те отрасли, которые стали фактическими бенефициарами ситуации (доставка, e-commerce, игры и развлечения, образование), показали существенный рост. Кто-то, наоборот, снижал потребление сервисов, консервируя некоторые проекты и оптимизируя затраты. Поскольку среди наших клиентов почти отсутствует прослойка микробизнеса, а клиентская база хорошо дифференцирована по компаниям среднего и крупного бизнеса всех отраслей, для нас ситуация была скорее благоприятной. Сегмент рынка, к которому относятся наши клиенты, был готов к краткосрочным трудностям и продемонстрировал нацеленность на долговременный рост. Наши затраты остались практически прежними: конечно, пришлось увеличить количество платных лицензий Zoom, чтобы все сотрудники могли полноценно организовывать удаленные встречи. Но в то же время мы существенно сэкономили на командировках. До пандемии мы

Олег Ковернзев, операционный директор, «Яндекс. Облако»



ставили себе задачу расти почти на порядок быстрее среднерыночных показателей и намеченных темпов не уронили.

Вместе с тем на российском рынке стал заметен переход многих организаций к построению собственных цифровых отраслевых платформ и продуктов на базе внешних платформ. Сегодня во многих компаниях руководство осознало, что если они не будут менять бизнес-модель – создавать новые продукты, каналы привлечения клиентов, искать какие-либо бизнес-коллаборации, то их или «подвинут» на рынке, или просто «съедят». В регионах, конечно, процесс идет немного медленнее, в первую очередь из-за ограниченного пула специалистов, способных интегрировать облачные технологии в рабочие процессы компании. Положительную динамику можно отметить в сегменте компаний-разработчиков из регионов и, на удивление, в государственных организациях, где, с одной стороны, есть бюджетные ограничения, а с другой – появились региональные метрики цифровизации, и ускоренное внедрение прикладных сервисов на базе облачной платформы становится реальной альтернативой классическому подходу. Так что «цифровую продуктизацию» бизнеса и уход от негибких готовых решений в сторону создания собственных (в том числе на базе open source) можно назвать тенденцией, которую мы явно увидели именно в 2020 г.

Краткосрочные эффекты пандемии уже закончились, но многие решения, которые приняты в компаниях, отмене не подлежат. COVID-19 ускорил запуск некоторых проектов и изменил паттерны потребления и людей, и компаний. Например, в Татарстане на базе трех медучреждений внедрили систему помощи для врачей. С технологической точки зрения это система распознавания снимков КТ, которая запущена по модели SaaS у нас в облаке вместе с партнером RadLogics. Благодаря решению время описания снимка врачом сократилось в шесть раз. Этот сервис будет масштабироваться, так как доказал свою полезность в сложное время. Другой пример – доставка продуктов. Один из наших клиентов – компания «СберМаркет» – последние полгода демонстрирует рост, и я уверен, эта тенденция продолжится уже вне зависимости от ограничительных мер, поскольку процесс запущен.

Облачная платформа как фундамент

PaaS – это больше, чем услуга, это набор интегрированных между собой сервисов, которые являются не просто «ресурсом по запросу», а инструментом, дающим компаниям возможность создавать собственные продукты и сервисы на надежном фундаменте. И этот инструмент постоянно развивается. Одно из самых перспективных направлений развития – бессерверные (serverless) вычисления. Это не сопутствующая услуга, а новая модель потребления ресурсов в облаке. Фактически это платформа в платформе, которая имеет целый ряд преимуществ:

- она берет на себя всю работу по обеспечению надежности и отказоустойчивости. Для небольших компаний это хорошее подспорье, так как квалифицированные специалисты, которые умеют это делать, стоят дорого;

- предоставляет интеграцию с большим количеством сервисов облака. Это прямое снижение расходов на разработку – вместо того чтобы изучать, как работать с теми или иными сервисами, и писать довольно шаблонный код, можно сфокусироваться на разработке бизнес-логики и уменьшить за счет этого время вывода продукта на рынок;
- обеспечивает автомасштабирование «из коробки». Система разработана так, что заботиться об этом вообще не надо, – она сама подстраивается под профиль нагрузки;
- позволяет прогнозировать стоимость обработки данных с высокой точностью и линейной масштабируемостью в зависимости от их объема, в отличие от обработки с помощью Hadoop или собственных решений на основе виртуальных машин;
- использует модель оплаты pay as you go – оплачивается только реальное потребление ресурсов, а не резерв мощностей. В случае колебаний объема трафика (как сезонных, так и суточных) экономия может быть существенной, поскольку гранулярность масштабирования и оплаты куда меньше, чем у традиционных решений с виртуальными машинами, а скорость, с которой система реагирует на изменение нагрузки, куда выше (секунды против единиц минут).

Мы видим востребованность облачной платформы. Уже сейчас на сервисы PaaS приходится почти половина нашей выручки, и доля может еще вырасти. Думаю, что дополнительный рост возможен как раз за счет увеличивающейся популярности serverless-сервисов. Кроме того, хочется выделить растущую востребованность надежных и функциональных управляемых сервисов баз данных и Kubernetes. Это одни из самых быстро развивающихся сервисов. Также можно отметить популярность сервисов распознавания и синтеза речи, особенно в сценариях роботизации колл-центров.

PaaS в Сбербанке

Использование сервисов PaaS повышает эффективность и сокращает время разработки новых продуктов в самом крупном банке страны.

Евгений Колбин, вице-президент, ПАО «Сбербанк», генеральный директор, SberCloud

Цифровая платформа Сбербанка

Сбер активно применяет в своей работе облачную Цифровую платформу Сбербанка (ЦПС). Она представляет собой комплекс средств и архитектурных шаблонов проектирования приложений, инструментов разработки, тестирования, развертывания и мониторинга, а также включает набор технологических и базовых прикладных сервисов.

ЦПС – это собственная разработка Сбербанка, которая базируется на большом количестве open source-решений, благодаря чему ускоряется создание новых возможностей ЦПС и в то же время прикладные команды изолируются от системной реализации за счет фиксированных контрактов. Сбербанк постоянно отслеживает тренды рынка open source, как крупных игроков, так и небольших проектов, и при появлении новых эффективных решений может быстро включить их в свою платформу.

Использование облачной платформы дает возможность перейти от простого потребления инфраструктурных сервисов к более эффективной облачной модели, микросервисной архитектуре, а также к созданию приложений и сервисов cloud native. PaaS позволяет получить «внутреннюю» выгоду в виде ускорения процессов разработки, повышения гибкости и эффективности бизнес-процессов и ИТ-систем (они становятся дешевле и продуктивнее). Теперь нет необходимости тратить усилия разработчиков на создание системных механизмов (например, проверку прав доступа, журналирование, аудит и многое другое) – все это доступно в платформе. Прикладной разработчик концентрируется на своей основной задаче – написании бизнес-логики.

Применение ЦПС дает и прямые преимущества для основного бизнеса банка. Речь идет о более быстром тестировании маркетинговых гипотез и кардинальном ускорении создания/внедрения/вывода на рынок новых продуктов и услуг.

PaaS от SberCloud

У входящей в экосистему Сбербанка компании SberCloud существует своя линейка платформенных сервисов под названием SberCloud. Advanced. Она включает в себя 40 облачных сервисов, которые предоставляют пользователям возможность реализовать практически любые ИТ-сценарии.

С помощью платформы SberCloud.Advanced можно создавать облачные продукты и сервисы в самых разных областях экономики, науки

и образования: от простых систем резервного копирования и ИТ-инфраструктуры целых предприятий до развертывания «умных» систем электронной коммерции, аналитики на основе искусственного интеллекта и платформ дистанционного обучения. Например, используя сервисы SberCloud.Advanced, можно создать «умный» отказоустойчивый интернет-магазин, который выдержит любой наплыв пользователей даже в «черную пятницу» и при этом предоставит всю необходимую бизнес-аналитику.

Платформенные сервисы SberCloud.Advanced позволяют быстро получить требуемую ИТ-платформу (или несколько), полностью готовую к работе. Например, при использовании базы данных PaaS разработчики буквально через 10 минут смогут загружать данные в новую базу данных и выполнять запросы к этим данным. Важно, что процессы создания и удаления новых экземпляров баз данных не требуют глубоких специфических знаний и выделенных администраторов, что соответствует таким актуальным ИТ-практикам, как DevOps. Кроме того, большую часть задач сопровождения платформ, включая резервное копирование, обновление и т.п., берет на себя SberCloud. Использование платформенных сервисов позволяет полностью автоматизировать многие процессы разработки и свести к минимуму фактор человеческой ошибки.

Облачная платформа – это живая система. Регулярно выходят обновления существующих сервисов, разрабатываются и добавляются новые. Как у любого продукта, у платформы есть дорожная карта развития. В ближайших планах – создание мультимодальных интерфейсов, расширение low code-сегмента и маркетплейса, на котором сторонние разработчики смогут размещать решения, созданные на платформе Сбербанка. Многие сервисы облачной платформы, которые в настоящий момент используются в Сбербанке, станут доступны внешним клиентам.

Импортозамещение в PaaS

Законодательные риски склоняют международные компании к тому, чтобы при работе в России использовать сервисы PaaS отечественных облачных провайдеров. На вопросы издания отвечает Александр Дорофеев, руководитель Big Data компании «Ашан Ритейл Россия».

– Александр, говорят, что у компании «Ашан» был опыт работы с облаком Google, но в итоге от сервисов глобального облачного провайдера отказались. Почему?

– Действительно, Auchan Retail выбрал облачную платформу компании Google для разработки и развертывания аналитических решений. Однако законодательства разных стран отличаются друг от друга, иногда существенно. Это, безусловно, основной риск при выборе глобального решения для любой международной компании, к числу которых относится и Auchan. Когда мы совместно с нашими коллегами из Auchan Retail оценили плюсы, минусы и риски использования облачной платформы Google для «Ашан Россия», то приняли решение развивать аналитическую платформу одного из российских облачных провайдеров.

Проанализировав предложения на российском рынке, мы выбрали облачную платформу от компании Mail.ru, поскольку она, по нашему мнению, лучше всего отвечает функциональным и техническим требованиям, которые мы предъявляем к своей аналитической платформе Auchan Big Data Platform.

В настоящее время мы используем платформу Mail.ru Cloud Solutions для развертывания всех компонентов, которые входят в Auchan Big Data Platform: Hadoop 3, GreenPlum, Clickhouse, Kubernetes. Также мы задействуем S3 для хранения архивных данных и GitLab для CI/CD. Все сервисы мы потребляем по модели PaaS. Это позволяет нам сконцентрироваться на разработке AI-решений для бизнеса, в то время как вопросами технической поддержки серверов и кластеров занимаются специалисты Mail.ru.

– В чем плюсы и минусы использования Paas? Какие возникали проблемы?

– Потенциальных минусов у PaaS, на наш взгляд, всего два – отсутствие контроля над вычислительной инфраструктурой (по сравнению с IaaS) и более низкая скорость доступа к данным по сравнению с локальными системами.

В то же время плюсов, считаю, у модели PaaS для нас существенно больше. Перечислю наиболее важные из них.

Во-первых, высокая скорость развертывания всех необходимых нам компонентов и технологий позволяет команде Big Data сразу приступить к разработке AI-решений. Причем в рамках PaaS мы получаем компетентную техническую поддержку всех сервисов, что тоже немаловажно, особенно с учетом сложности поиска специалистов в сфере Big Data и их стоимости на рынке.

Второй важный для нас фактор – возможность масштабирования компонентов в любой момент времени, что позволяет нам быстро увеличивать вычислительные мощности при необходимости, например, при запуске новых AI-решений. Так как мы платим только за потребляемые ресурсы, это помогает достигать более высоких показателей возврата инвестиций по нашим проектам.

В-третьих, затраты на аренду облачной платформы в течение трех-пяти лет ниже затрат на закупку серверов и кластеров для собственного ЦОДа. Кроме того, при закупке оборудования есть риск ошибки в расчете оптимальной конфигурации аппаратного обеспечения, в то время как при работе в облаке всегда можно провести перебалансировку ресурсов с учетом новых требований, оставаясь при этом в рамках запланированного бюджета. Например, для одного из наших решений на основе машинного обучения потребовалось больше RAM и меньше CPU по сравнению с тем, что мы первоначально предполагали. Когда мы это поняли, в течение часа скорректировали конфигурацию кластера, что повысило производительность нашего решения в сфере машинного обучения. Но расходы на кластер при этом не выросли.

– Каковы ваши планы по развитию PaaS-сервисов?

– В рамках нашей стратегии в ближайший год мы планируем разработать и запустить новые AI-решения, которые помогут нам реализовать инновационные проекты. Это решения в сфере логистики, ценообразования, оптимизации ассортимента, персональных сервисов для покупателей и безопасности (противодействия мошенническим действиям). Некоторые из этих решений потребуют включения в архитектуру Big Data Platform новых компонентов, и мы уверены, что с помощью PaaS сможем быстро и качественно их развернуть.

Беседовал Николай Носов

Кто и для чего использует PaaS?

Вендоры могут долго рассказывать о преимуществах своих облачных сервисов. Но гораздо интереснее послушать людей по другую сторону прилавка.

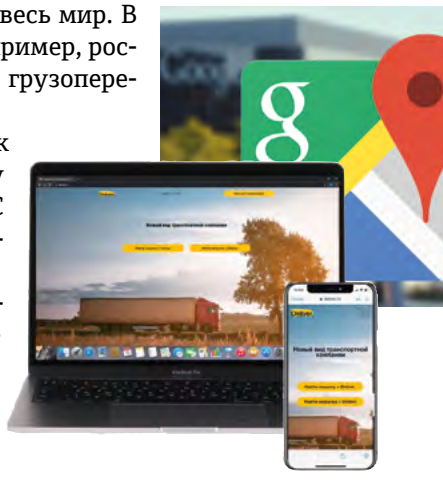
Николай Носов

Чтобы выяснить, как компании в России работают с облачными платформенными сервисами, «ИКС-Медиа» совместно с iKS-Consulting летом 2020 г. провели опрос пользователей PaaS-решений и изучили конкретные примеры. Поскольку границы между IaaS и PaaS, PaaS и SaaS нечеткие, приходилось уточнять, что понимает под PaaS тот или иной эксперт. Иной раз оказывалось, что компания совсем не использует облака, а под PaaS понимает средство разработки, установленное в офисе на виртуальной машине.

Тем не менее пользователи PaaS-сервисов в стране есть, есть и положительный опыт работы с ними. В числе поставщиков PaaS-услуг респонденты называли Amazon Web Services, Microsoft Azure, Mail.ru Cloud Solutions, «Яндекс.Облако», Oracle Cloud и Google Cloud Platform.

Пользователи ведущих мировых гиперскейлеров (AWS, MS Azure) плюсами их PaaS-услуг считают широкий функционал, быстроту и легкость развертывания, гибкость, простоту масштабирования.

Козырь Google – картографическая система Google Maps, охватывающая почти весь мир. В России с ней успешно работает, например, российская компания онлайн-сервиса грузоперевозок Deliver.



Плюс Oracle Cloud – простой доступ к СУБД Oracle, которая по-прежнему популярна на российском рынке. С PaaS-сервисами Oracle работают «Ингосстрах», Schneider Electric, Tele2.

Конкурентные преимущества отечественных облачных провайдеров – соответствие требованиям российских регуляторов и оплата в рублях. Да и служба поддержки, как правило, работает лучше. По

функционалу отставание от ведущих мировых гиперскейлеров есть, но оно стремительно сокращается.

Недочеты и недоработки

Респонденты рассказали о возникающих при использовании облачных платформ сложностях. «Проблемой стала миграция в облако из on-premise. Пришлось переделывать ряд программ для работы с S3-хранилищем, у которого есть функции, по-разному реализованные разными облачными провайдерами. После доработки программы перестали зависеть от облачной платформы, так что при необходимости мы сможем поменять облачного провайдера», – отметил Григорий Никонов, управляющий директор диджитал-агентства Wunderman Thompson Moscow.

К лидерам – AWS и Microsoft Azure – особых претензий нет, но у AWS нет представительства в России, что затрудняет взаимодействие. Кроме того, ценообразование у гиперскейлера непрозрачное: итоговый счет может существенно отличаться от планируемого. К недостаткам Microsoft Azure можно отнести слабую поддержку кириллицы.

Юлия Бедросова, руководитель, «Web-студия Юлии Бедросовой»

> Облачные решения нужно уметь «готовить». Самое сложное – расчет стоимости. Хотя AWS предоставляет калькулятор, оценки получаются очень приблизительными. Фактическое использование сервисов не всегда совпадает с ожидаемым. В итоге пара месяцев может уйти на дополнительную настройку сервисов, чтобы укладываться в бюджет.

По словам одного из бывших топ-менеджеров крупной международной ритейл-компании, Google, в отличие от других гиперскейлеров, практически не идет навстречу даже крупным клиентам, не включает их пожелания в карту развития продуктов, медленно устраняет выявленные ошибки. Кроме того, по утверждению эксперта, Google не дает финансовых преференций даже при большом объеме потребляемых сервисов.

Несколько респондентов перешли на сервисы российских PaaS-провайдеров. При этом они отмечали значительно меньший их функционал по сравнению с облаками западных гиперскейлеров. По поводу лидирующих российских PaaS-провайдеров мнения разделились. Выделяли PaaS-сервисы Mail.ru Cloud Solutions и «Яндекс.Облако», но пальму первенства отдавали, исходя из стоящих перед компанией задач.

Несомненные успехи

Компании поделились и примерами успешного использования облачных платформенных сервисов. Так, российская компания 2ГИС разрабатывает мобильные офлайн-карты, с которыми можно найти почти любую компанию более чем в 500 городах мира. Над продуктом, которому доверяют около 50 млн человек в месяц, работают свыше 4,5 тыс. специалистов. Они находятся в разных городах, но обращаются к внутренним программным продуктам, созданным 2ГИС и включенным в ее единую ИТ-инфраструктуру. Решать технические вопросы помогает служба поддержки – она получает более 200 обращений в день. До недавнего времени инциденты классифицировались вручную. Однако после развертывания службы машинного обучения Microsoft Azure командам внутренней техподдержки 2ГИС удалось высвободить 70 ч рабочего времени в месяц на каждого ИТ-специалиста, при этом решение вопросов ускорилось на 20%.

Базы данных, файловые хранилища, балансировщики нагрузки, Kubernetes, DNS-сервисы и многое другое использует в облаках AWS, Google Cloud Platform и «Яндекс.Облако» компания Voximplant. Технический директор и сооснователь занимающейся облачными коммуникации компании Андрей Коваленко отметил, что переход на PaaS упростил жизнь и сделал процессы более эффективными, так как специалисты занимаются тем, чем и должны заниматься, – разработкой продукта, а не обслуживанием инфраструктуры.

Диджитал-агентство Wunderman Thompson Moscow работает в России с 1997 г. Компания разрабатывает сайты, занимается рекламой и консалтингом. С самого начала она ориентировалась на продукты Microsoft и при появлении MS Azure стала ее пользователем. Однако необходимость выполнять положения законодательства о защите персональных данных заставила искать российского облачного провайдера. Требования к облачной платформе предъявлялись следующие: плата только за потребляемые ресурсы, отличная работа с продуктами Microsoft, наличие базового набора инструментов, включая балансировщик нагрузки и резервное копирование. Сегодня компания использует Kubernetes в облаке Mail.ru Cloud Solutions. PaaS-сервисы значительно повысили эффективность рабочих процессов, поскольку низкоуровневые сервисы стали проблемой облачного провайдера. По словам Г. Никонова, техподдержка находится на должном уровне:

«Оперативно решаем любые вопросы в Telegram-чате. В любое время суток и в режиме одного окна».

Компания «Газпром межрегионгаз Ухта», поставляющая природный газ потребителям Республики Коми и Архангельской области, приняла решение ускорить процесс ввода передаваемых по телефону показаний газовых счетчиков. Был выбран PaaS-сервис распознавания и синтеза речи из портфеля «Яндекс.Облако». С его помощью в настоящий момент обрабатываются 75% звонков, и время приема показаний сократилось вдвое.

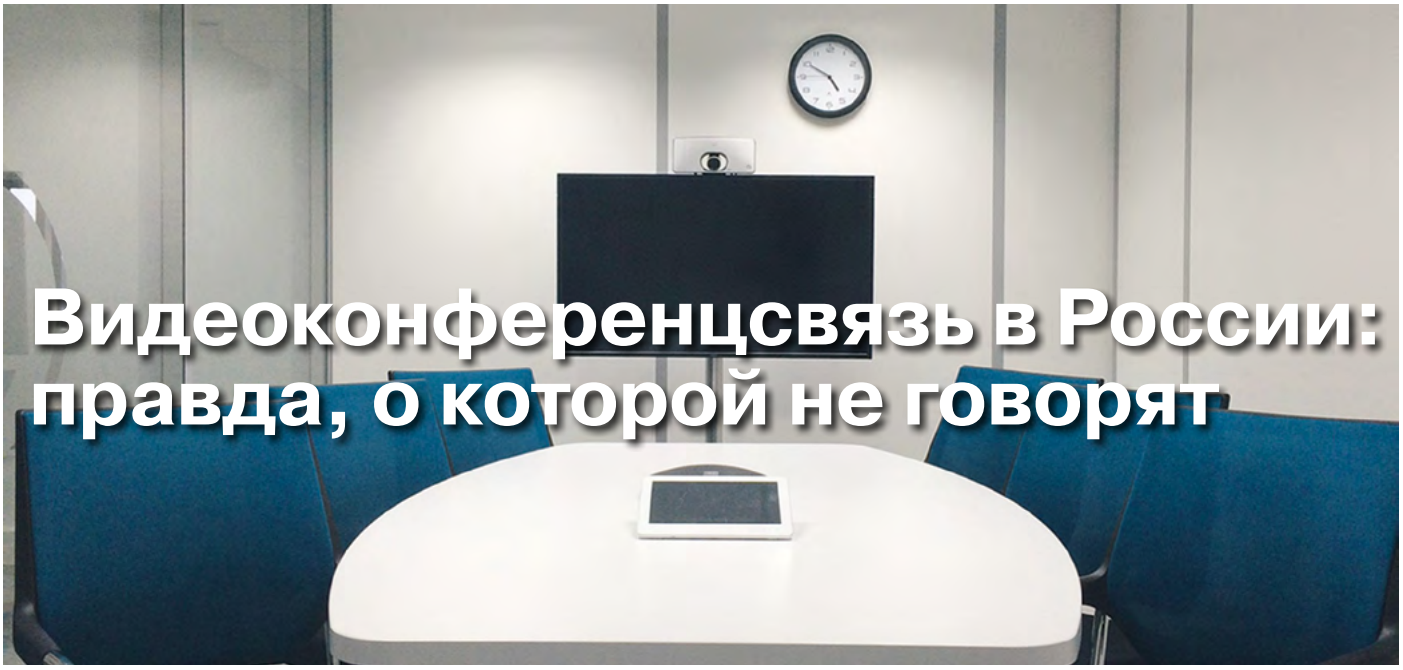
Представители банков и страховых компаний видят эффект от внедрения PaaS-решений в сокращении времени разработки приложений и вывода продуктов на рынок, уменьшении трудозатрат на администрирование и поддержание кластеров в рабочем состоянии, а также в снижении расходов. «Каждую неделю мы выпускаем новые релизы наших систем, поэтому быстрая и надежная разработка ПО, возможность оперативно увеличить пул ресурсов, эффективно и быстро управлять тестовыми средами для нас критична. Мы используем метод управления проектами scrum, в рамках которого продукт разрабатывается в ходе нескольких итераций (спринтов), разбивающих сложные проекты на небольшие задачи. Нагрузка на тестовые среды в течение спринта (10 рабочих дней – две недели) минимальна, за исключением демодня (конец спринта). Поэтому нам выгодны сервисы, которые в обычное время почти ничего не стоят и платить за эксплуатацию которых надо лишь в демодни», – рассказал Алексей Клепиков, вице-президент по информационным технологиям «Ингосстраха».

Ритейл-компании отметили, что использование PaaS привело к снижению затрат на инфраструктуру и одновременно резкому увеличению количества пилотируемых проектов. Эксперты из промышленности выделили сокращение времени на сбор данных для прогнозов и ускорение ключевых бизнес-процессов.

Дороги для всех

Всего год назад поиск удачных примеров использования PaaS в российских компаниях был непростой задачей, однако ситуация сильно изменилась – пандемия подстегнула переход на облачные платформы. Провайдеры выдержали повышение спроса и в основном смогли оправдать ожидания клиентов.

В дальнейшем одни облачные провайдеры будут улучшать существующие «пути», делая «езду» клиентов более простой и комфортной. Другие – нащупывать новые тропинки, стараясь предугадать запросы клиентов и опередить конкурентов на новых направлениях. Но можно сказать с уверенностью – «дорог» хватит на всех. ИКС



Видеоконференцсвязь в России: правда, о которой не говорят

Борис Попов, директор по развитию бизнеса, Vinteo

Сегодня сотрудники многих компаний продолжают работать удаленно, и российский рынок видеокоммуникаций остается в зоне повышенного внимания. Однако эксперты рынка зачастую опускают вопросы классификации систем видеосвязи и тем затрудняют грамотный выбор решений.

Классы систем видеосвязи

Разговор о рынке видеообщения следует начать с выделения трех основных классов технологий, которые на нем присутствуют. Важно отметить, что решения, относящиеся к разным классам, имеют разные преимущества и ограничения, используют разные технологии, поддерживают разный функционал и качество видеосвязи, предназначены для разных задач и в общем случае технически несовместимы между собой.

Видеоконференцсвязь (ВКС). Эта технология предназначена для обеспечения бизнес-процессов и передачи критичных к качеству потоков видео и аудио, когда участники в режиме видеоконференции обсуждают свои вопросы, используя ВКС как инструмент. При этом пользователи имеют гарантированное качество видео и звука, без задержек и искажений, всегда видят необходимых абонентов и докладчиков, получая так называемый эффект присутствия. Количество абонентов ВКС может быть практически неограниченным.

Видеоконференцсвязь базируется на общепринятых стандартах и рекомендациях Международного союза электросвязи, благодаря чему становится возможным взаимодействие оборудования разных производителей; для кодирования и декодирования потоков с целью уменьшения задержек задействуются специальные устройства (кодеки). Абонентским комплектом может служить персональный компьютер, однако использовать беспроводные каналы связи, мобильные устройства и т.д. рекомендуется только в качестве резервных или аварийных. Эта технология требует более серьезных вложений в инфраструктуру по сравнению с другими классами: необходимо оборудовать залы, переговорные комнаты и рабочие места абонентов и, главное, – установить достаточно мощные серверы MCU (Multipoint Control Unit). Серверы MCU обрабатывают сотни и тысячи видеопотоков от подключенных абонентов и отдают каждому из них готовую персональную «картинку» в одном потоке аудио и видео, что обеспечивает значительно более высокое качество передачи видео и звука по сравнению с решениями других классов.

Вершина развития ВКС – технология Telepresence, полного погружения человека в общение с собеседником с достижением эффекта контакта «глаза-в-глаза». Здесь не только используются самые высокие характеристики передачи видео и звука из арсенала доступных в ВКС, но и уделяется особое внимание подготовке помещения (установка студийного звука, света, фона и даже специальная расстановка мебели). Такой подход создает эффект полного присутствия:

участники общаются так, как будто находятся в одном помещении, и забывают о существовании между ними технических средств, концентрируясь на обсуждаемой тематике.

Вебконференцсвязь получила массовое распространение при активном развитии интернета. Она основана на передаче одного и того же изображения всему массиву подключенных абонентов, но с разным качеством. В качестве терминалов задействуются в основном персональные компьютеры, планшеты и смартфоны. Абонентское устройство каждого из участников из всех потоков выбирает тот, который в состоянии обработать, и выводит его на экран, принимая, но игнорируя остальные потоки. Данный сегмент исторически предназначался для работы в малых группах (до 50 абонентов).

Вся обработка видео и формирование итоговой «картинки» вместо сервера MCU выполняется процессором абонентского устройства, а центральный сервер занимается только коммутацией потоков аудио и видео. При этом каждый из производителей применяет собственные протоколы сжатия и передачи потоков аудио и видео (для улучшения сжатия и уменьшения задержек). Оборотной стороной перехода на проприетарные протоколы является невозможность взаимодействия систем разных вендоров, а качество видео и звука никак не контролируется и не гарантируется системой.

При отображении на экране нескольких выступающих сервер отправляет каждому из зрителей соответствующее количество видеопотоков. В результате на экране редко присутствуют более четырех-пяти докладчиков, а качество изображения и звука напрямую зависит от сценария проводимого мероприятия. Как правило, вебконференцсвязь используется для онлайн-лекций, когда докладчика с презентацией слушает множество абонентов. Возможность вывести определенного абонента на экран для того, чтобы он мог подать реплику или задать вопрос, при этом либо исключается, либо технически ограничена, взаимодействие аудитории и выступающего происходит в основном при помощи чата.

Видеокоммуникатор. Это технология видеообщения «точка – точка», или просто видеотелефон. При организации многоточечной связи раскладка абонентов только одна, количество собеседников на экране не превышает 10–12.

Рынок в тумане

Российский рынок видеоконференцсвязи был сформирован в 2000-х гг. ведущими зарубежными игроками – производителями систем ВКС профессионального класса. Отечественных решений на нем практически не было. На тот момент в нашей стране технология была неразвита. Поскольку системы ВКС были дорогими и сложными, их могли позволить себе в основном крупные государственные и коммерческие структуры. Они и стали основными заказчиками систем видеоконференцсвязи, сформировав этот небольшой сегмент ИТ-рынка. Фактически 90% сетей ВКС были построены на оборудовании иностранных вендоров, среди которых наибольшей популярностью пользовались Avaya, Cisco Systems, Polycom (ныне – Poly).

Однако программа импортозамещения и контрсанкций, введенная в действие после 2014 г., привела к появлению на рынке отечественных

Занятия по физике для школьников, г. Гагарин ▼

Фото: Vinteo

производителей систем видеосвязи: IVA Technologies, Mind, SPIRIT, TrueConf, Vinteo и др. Многие из них пошли по пути разработки решений в сегменте веб-конференций. Это объяснимо, так как подобные системы более просты с технологической точки зрения, зачастую основываются на использовании open source-продуктов и не предъявляют особых требований к серверному оборудованию.

Но продавать эти упрощенные продукты некоторые вендоры начали в качестве полноценных систем ВКС профессионального класса, заявляя об их соответствии единому списку технических стандартов ВКС и говоря об успешном и недорогом импортозамещении в этом сегменте. Поскольку веб-конференция – другая технология, полноценно интегрироваться с имеющейся инфраструктурой ВКС профессионального класса она не может. Часто заказчик, уже инвестировав в проект и приобретя (как ему казалось – очень удачно) дешевое отечественное решение ВКС, сталкивается с тем, что при интеграции такого продукта в существующую инфраструктуру система в целом не функционирует. Новый сегмент сети работает отдельно и требует отдельной поддержки и обслуживания.

Рынок программных и аппаратных средств видеосвязи перенасыщен самыми разными по цене и качеству решениями поставщиков – от дорогостоящих переговорных комплексов до бесплатных программных сервисов. Однако не разработаны четкие процедуры оценки соответствия решений стандартам ВКС. Из-за этого во многих ведомствах системы ВКС, которые должны работать в единой сети по всей стране, несовместимы между собой, и это тормозит развитие таких важных направлений, как телемедицина, дистанционное образование и т.п.

Вместе с тем в сегодняшних обзорах рынка видеокоммуникаций, как правило, отсутствует разделение решений на классы, вендоры и интеграторы приводятся единым списком. Являясь представителем одного из российских производителей систем ВКС, воздержусь от классификации и ранжирования решений коллег и я. Такой анализ – задача для независимого исследования, потребность в котором становится все более настоятельной, поскольку отсутствие четкой классификации затрудняет подбор оборудования для проектов создания и особенно – расширения систем видеоконференцсвязи.

Как правильно выбрать решение?

На вопросы, связанные с выбором продукта видеосвязи, сложно ответить однозначно – это все еще проектный бизнес, и оптимальное решение зависит от поставленной задачи и имеющейся инфраструктуры, особенно для сетей федерального уровня.

Так, для системы на 50 пользователей видео в одноуровневой сети и при широких каналах связи прекрасно подойдет недорогое решение веб-конференций, и нужно только выбрать из многообразия производителей. Если же требуется система на 100 и более пользователей с задачей объединить новое решение с имеющимся «зоопарком» оборудования, с территориально разнесенными узлами, узкими или нестабильными каналами – тут круг игроков резко сужается до классических «железных» решений или программных ВКС профессионального класса. Такие решения, даже отечественного производства, потребуют заметных инвестиций, но они необходимы для расширения «серьезных» систем ВКС, использующих каскадирование серверов, транки, систему управления вызовами, транскодирование «картинки» на стороне сервера и др.

Стоит отметить, что сегодня среди систем профессионального класса практически отсутствуют моновендорные сети – как правило, требуется объединять сегменты разных вендоров с разными задачами. В результате введения режима самоизоляции изменилась структура абонентов профессиональных сетей ВКС. Подавляющее большинство абонентов для участия в сеансах ВКС перешли на программные клиенты для персональных компьютеров и мобильных клиентов, резко повысилось количество одновременных участников конференций. Стандартными кодеками продолжают пользоваться не более 10–15% абонентов из больших залов заседаний и переговорных комнат.

Рассмотрим, как должна выглядеть схема внедрения профессионального решения видеосвязи. Например, у государственной организации ранее установлено оборудование ВКС нескольких иностранных вендоров, и пришло время масштабировать или обновлять сеть. Цель – получить единую систему видеосвязи, в которой новые и старые компоненты будут слаженно работать, обеспечивая нужный функционал. При этом надо сохранить возможность для дальнейшего масштабирования сети и желательно сэкономить бюджет.

У заказчика есть два пути – обратиться к зарубежным вендорам, на оборудовании которых построена имеющаяся сеть ВКС, или выбрать отечественное решение. Если заказчику необходимо соблюсти все условия импортозамещения, то он начинает искать продукты отечественного производства, при рассмотрении предложений обращаясь к единому списку технических стандартов видеосвязи, которые они должны поддерживать.

Самый действенный способ проверки отобранных вариантов – установка пилотного ре-

шения ВКС на базовой сети организации и тестирование продукта в рабочих условиях. Пилотная эксплуатация позволит определить реальный функционал решения и покажет готовность вендора к честной работе до заключения контракта. Также желательно сразу узнать, как будет происходить обслуживание системы ВКС после покупки. Заказчик должен получить поддержку от специалистов, которые хорошо знакомы с реалиями российских проектов и смогут в случае необходимости переписать ядро системы. И только если продукт соответствует техническим требованиям и к его предпродажному тестированию замечаний нет, можно подписывать контракт на поставку.

Реалии импортозамещения в ВКС

Как было сказано выше, госполитика и санкции в 2014 г. сильно повлияли на рынок ВКС в России и дали отечественным разработчикам карт-бланш на вывод на рынок своих решений. Но поскольку некоторые вендоры выступили за нивелирование технологических различий между классами решений видеосвязи, у заказчиков появился негативный опыт в использовании так называемых систем ВКС (по сути – упрощенных решений веб-конференций), а следовательно, и стойкое убеждение, что российских аналогов продуктов Cisco, Polycom и других не существует. Эту идею растиражировали СМИ и эксперты, увидев иностранное решение ВКС у президента, и в итоге даже от правительства посыпались предложения по созданию «убийцы» условного Zoom.

В реальности ситуация несколько иная. Во-первых, если говорить об использовании иностранных решений ВКС в больших государственных ведомствах, где вся инфраструктура изначально была построена на их продуктах, то нужно понимать, что масштабная замена парка оборудования требует времени и внедрение новых решений в некоторых случаях занимает годы.

Во-вторых, российских решений ВКС, которые поддерживают стандарты традиционных систем видеоконференцсвязи (включая H.323 и SIP), совместимы с системами Avaya, Cisco, LifeSize, Polycom и др. и которые можно внедрять в уже существующие сети, построенные на оборудовании этих вендоров, на рынке единицы. Однако немногочисленные российские решения, которые полностью соответствуют этим требованиям, уже достаточно широко используются в сетях крупных государственных заказчиков, обеспечивая полнофункциональную замену серверов Cisco и Polycom, поддержку более 100 участников, работу в закрытых сетях, отказоустойчивость, высокий уровень безопасности и др. Пока это не масштабные проекты, и многие заказчики все еще предпочитают иностранных вендоров, однако здравый смысл в вопросах цены и безопасности никто не отменял.

Фото: Vinteo

▲ **Урок физики в 1-м Московском кадетском корпусе**

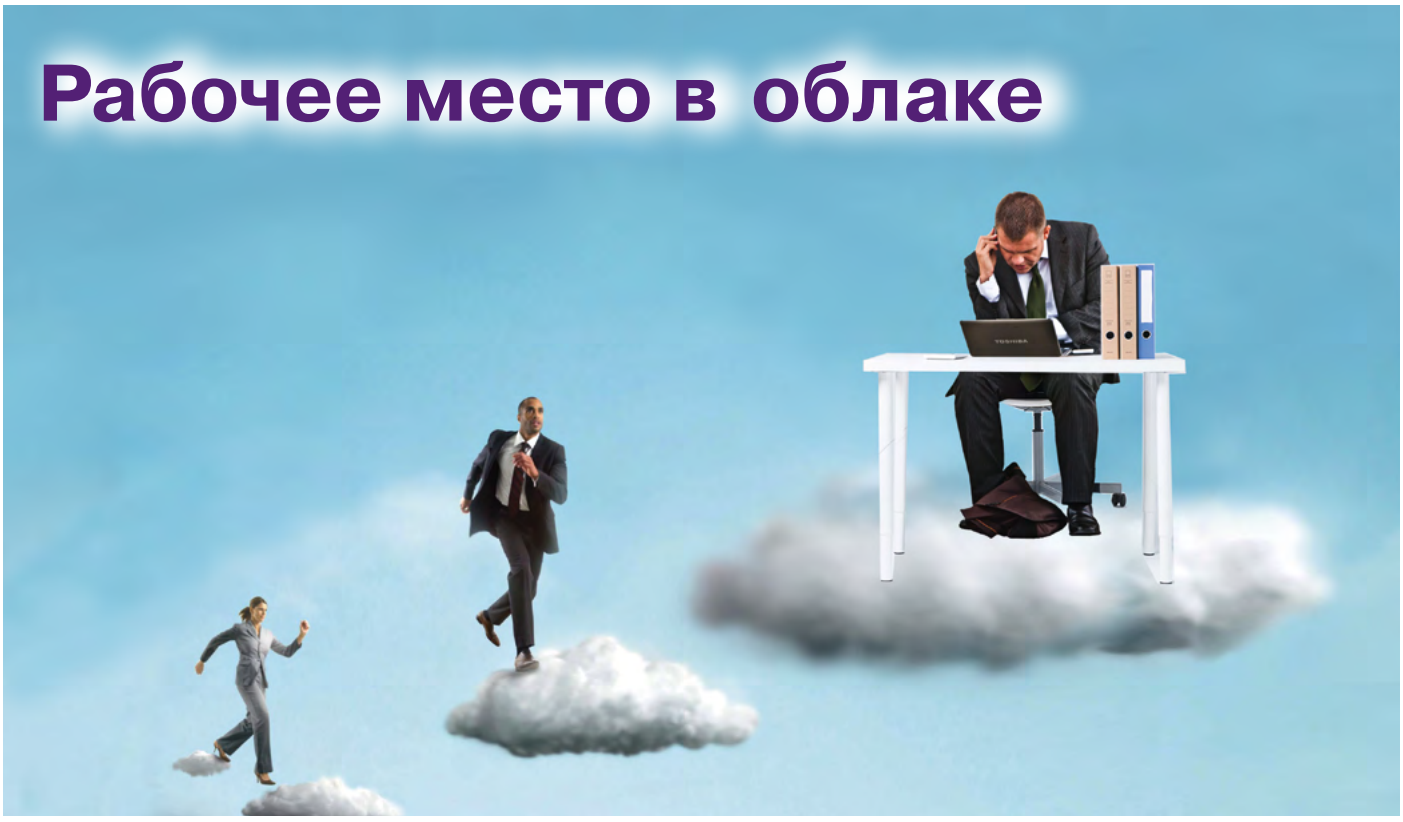
Например, реализация проекта ВКС на решении иностранного вендора, как правило, влечет за собой развертывание большого количества разных продуктов этого производителя (обычно отдельных аппаратных серверов со своим интерфейсом управления), требует достаточно дорогостоящей подписки на сервисы, а также наличия специалиста, который глубоко понимает инфраструктуру именно этого вендора и свободен для поддержки проекта. Размещение серверов в другой стране сразу остро ставит вопрос безопасности, и госструктуры не всегда могут себе позволить его обойти.

Инвестиции тоже имеют значение: масштабный отечественный проект ВКС в целом получится дешевле на 30–40% за счет как более низкой стоимости, так и отсутствия необходимости платить за дополнительный функционал.

Конечно, при желании заказчик всегда может обосновать использование именно иностранных решений, но все-таки тенденция внедрения отечественных продуктов ВКС набирает силу. Изначально этому поспособствовал закон об импортозамещении и определенные критерии для включения в реестр отечественного ПО, попадание в который дает преимущества при госзакупках. Если политика импортозамещения продолжится в этом русле, без принятия комплиментарных для иностранных вендоров поправок, то у отечественных разработчиков ВКС есть все шансы со временем потеснить иностранцев в большинстве проектов.

Среди очевидных преимуществ отечественных решений – возможность кастомизировать решение под любые пользовательские сценарии. Тем самым заказчик получает возможность приобрести широкий функционал системы, полное и бесшовное совмещение всех имеющихся систем аудио- и видеообмена между собой, а также прямую сервисную поддержку. ИКС

Рабочее место в облаке



Николай Носов

В условиях продолжающейся пандемии популярность сервисов удаленного рабочего места в облаке будет расти, хотя в России DaaS пока используют нечасто.

Новое – хорошо забытое старое

Идея удаленного использования вычислительных ресурсов не нова. Развитие ИТ – постоянная борьба концепций централизации, выполнения вычислений в одном узле, и децентрализации, когда каждый пользователь задействует свои вычислительные мощности.

На первых компьютерах работали по очереди, пользователь имел в распоряжении все устройство. Потом компьютеры начали поддерживать многозадачность и одновременную работу нескольких человек. Стандартная для 80-х годов прошлого века конфигурация – ЭВМ в оборудованном системами кондиционирования и пожаротушения машинном зале и отдельно расположенный дисплейный класс. Все вычисления проводились на мейнфрейме, а установленное в дисплейном классе оборудование служило для ввода и вывода информации.

Бум персональных компьютеров в конце 80-х качнул маятник обратно – каждый сотрудник имел свой компьютер, и по крайней мере в офисах опять торжествовала децентрализация.

Для обмена информацией персональные компьютеры начали объединять в локальную сеть. В 90-х завоевала популярность конфигурация локальной сети с выделенными серверами, на которых выполняли задачи, создающие повышенную вычислительную нагрузку. Пользователи работали с ними через локальную сеть с персональных компьютеров в режиме тонкого клиента. Тогда же появился термин «удаленный рабочий стол» – Microsoft стала использовать протокол Remote Desktop Protocol (RDP) для удаленной работы пользователя с сервером, на котором был запущен сервис терминальных подключений (Remote Desktop Service, RDS).

Рост производительности компьютеров привел к распространению технологий виртуализации. Появилась инфраструктура виртуальных рабочих столов (Virtual Desktop Infrastructure, VDI). В отличие от технологии RDS, в которой пользователи проводят одновременные RDP-сеансы на одной машине с серверной ОС, при использовании VDI каждый пользователь подключается к своей виртуальной машине со своей операционной системой.

В 10-х годах нынешнего века место сервера заняло облако, а доступ к удаленным вычислительным мощностям стал осуществляться через интернет. Распространение сервисных моделей в ИТ привело к появлению услуги «рабочий стол как сервис» (Desktop as a Service, DaaS).

DaaS – это по сути VDI, предоставляемая облачным провайдером по сервисной модели.

Принцип работы DaaS

При работе с DaaS пользователь, запустив приложение на своем мобильном или стационарном устройстве, через интернет обращается к шлюзу (брокеру) в облаке поставщика услуги. Шлюз проводит аутентификацию пользователя (например, с помощью Active Directory), посылает в нужное рабочее пространство, по запросу пользователя подключает к вычислительным ресурсам облачного провайдера или on premise-системам предприятия. Пользователь начинает сеанс и с помощью предложенного шлюзом десктопа работает со своей виртуальной машиной в однопользовательском режиме. Есть и более дешевые варианты, в которых несколько пользователей подключаются к одной виртуальной машине с серверной ОС (например, Windows Server) или формируется мультисессия Windows 10.

Популярные на рынке решения для организации DaaS – Azure Windows Virtual Desktop, Citrix Managed Desktops, Amazon WorkSpaces, VMware Horizon.

Преимущества DaaS

DaaS объединяет достоинства облачной модели и технологии VDI. Сервис обеспечивает гибкость – пользователи имеют доступ к одной и той же среде рабочего стола из любого места, где есть подключение к интернету. При этом облака позволяют быстро масштабировать рабочие места в зависимости от потребностей бизнеса, будь то слияние компаний, наем и увольнение сотрудников, развертывание или ликвидация филиалов.

DaaS обеспечивает безопасность доступа. Не нужно беспокоиться о настройке VPN, RDP-серверов и другой специальной инфраструктуры для удаленного доступа к рабочим станциям компании. DaaS предоставляет пользователям безопасную точку доступа и упрощает администрирование политик информационной безопасности.

Пользовательские данные хранятся в облаке и, следовательно, останутся доступными, даже если их локальные устройства выйдут из строя. Облачные провайдеры, как правило, могут позволить себе более современные, дорогие и эффективные средства защиты, чем пользователи, и имеют более квалифицированных специалистов по обеспечению информационной безопасности.

Работа не прервется в случае стихийных бедствий или антропогенных катастроф, так как не зависит от использования вычислительного оборудования клиента. Облако лучше защищено – надежный провайдер создает катастрофоустойчивые решения.

Инфраструктуру VDI из облака легко администрировать. У пользователя своя виртуальная машина – если что-то работает не так, многое можно подправить самостоятельно, не обращаясь к службе техподдержки сайта. При этом облачный провайдер занимается администрированием, обеспечивает хранение данных, резервное копирование, безопасность и обновление ПО. Облачный сервис снижает зависимость от цепочек поставок для доставки физического оборудования, необходимого для поддержания инфраструктуры настольных компьютеров. Не нужно приобретать рабочие станции для каждого нового сотрудника, менять вышедшие из строя платы и жесткие диски.

К преимуществам облачной модели относятся снижение CAPEX и прогнозируемость OPEX. Причем клиент платит только за используемые ресурсы в рамках месячной или годовой подписки.

Оборотная сторона медали

Чтобы пользоваться облачной услугой удаленного рабочего стола, в первую очередь нужен надежный канал доступа в интернет. Когда началась пандемия, многие выехали на дачи, где доступ в интернет только мобильный. Такой канал надежно работает далеко не везде, а периодически зависающий при нажатии клавиш клавиатуры компьютер раздражает и снижает производительность труда. Не говоря уже о том, что пользователям надо не только видеть картинку на экране, но и загружать данные и выводить результаты на печать.

Сервис DaaS удобен, но не дешев, особенно если внимательно подсчитать все расходы. Предприятие экономит на покупке и сопровождении дорогих производительных компьютеров (CAPEX) для рабочих станций, но тратит деньги на оплату услуг (OPEX). Кроме того, компаниям все равно приходится думать о рабочих местах сотрудников, пусть и удаленных, – покупать ноутбуки или настольные компьютеры, настраивать и сопровождать конечные устройства, обеспечивать их безопасность. Конечно, требования к ним не очень высокие, а выход из строя жесткого диска не приведет к потере корпоративной информации, но эти затраты все равно нужно учитывать, выбирая DaaS.

Большинство облачных удаленных столов работают под управлением ОС Windows, поэтому придется платить за лицензию, возможно, косвенно – через облачного провайдера. Если удаленные сотрудники тоже работают под Windows, то число лицензий увеличится вдвое. Крупные предприятия могут вести переговоры с Microsoft о скидках в рамках соглашения

Microsoft Products and Services Agreement, но дополнительных расходов не избежать.

DaaS – далеко не самый популярный облачный сервис, так что зачастую ИТ-командам клиентов не хватает экспертизы. Конечно, значительная часть работы по поддержке удаленных рабочих мест перекладывается на облачного провайдера, но встраивать сервисы в бизнес-процессы компании, согласовывать политики безопасности никто за конечного пользователя не будет.

При использовании стандартных облачных моделей текущие данные пользователей часто хранятся или дублируются на рабочих станциях, и авария на стороне облачного провайдера не приводит к их потере. Инфраструктура облачного провайдера, как правило, надежнее и безопаснее, чем у пользователя, но аварии все же случаются. DaaS подразумевает, что вся обработка идет в облаке, «все яйца складываются в одну корзину», поэтому уровень доверия к облачному провайдеру должен быть высоким.

Сценарии использования DaaS

В некоторых сценариях DaaS выглядит наиболее привлекательно. Прежде всего, в ситуации, когда компании предоставляют доступ к вычислительной инфраструктуре постоянно меняющимся сотрудникам или партнерам, которые могут находиться даже в разных городах. Так происходит при создании филиалов, обменных пунктов, удаленных касс банков, при предоставлении временного доступа аудитору или ограниченного доступа быстро меняющимся сотрудникам колл-центров. Еще один вариант – учебные классы с переменным числом учащихся. С помощью DaaS новые рабочие места создаются и удаляются быстро и безопасно.

Да и администрировать такие места легче – автоматическое обновление рабочих мест не проблема и при традиционной архитектуре, но вот сделать «откат» в случае выявления ошибок будет непросто, придется исправлять их вручную. В случае DaaS достаточно вернуться к предыдущей версии в облаке.

Сервис интересен компаниям, уделяющим повышенное внимание информационной безопасности, например, из финансовой сферы. Данные не хранятся на локальных устройствах пользователей, тонкому клиенту запрещается использование флешек, и службам ИБ проще предотвратить утечку информации. Фотографируя экран, много данных не утащишь. Облегчается и администрирование доступа пользователей для служб ИБ.

Локальные рабочие станции могут стоить дорого, например, графические станции для 3D-моделирования. Зачастую дешевле получить услугу в облаке, чем покупать графическую станцию для каждого сотрудника, особенно если это приходится делать в кредит, когда начисляются проценты, а стоимость купленного оборудования уменьшается каждый день из-за морального устаревания. И уж точно это дешевле, чем покупать суперкомпьютер, доступ к которому в облаке также можно обеспечить через DaaS.

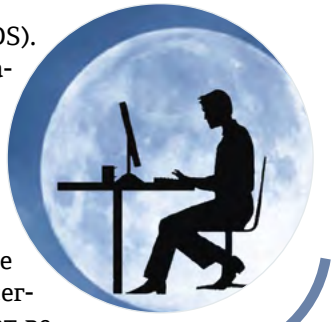
Направления развития DaaS

Удаленные рабочие места становятся все более «умными» и персонализированными. Современное удаленное рабочее место выступает помощником человека. Так, Citrix Workspace на основе анализа клиентского опыта формирует индивидуальный интерфейс, помогающий пользователю. Решение оптимизирует доступ к приложениям и даже предугадывает дальнейшие действия человека, оценивая их вероятность. Такие рабочие места повышают производительность труда сотрудников, подсказывают правильные алгоритмы и максимально автоматизируют операции.

Интеграция с устройствами IoT поможет сделать максимально комфортным и физическое рабочее место. Скажем, автоматически настроить высоту кресла, яркость и цветовую температуру настольного светильника, как это демонстрировалось на конференции Citrix Synergy 2019.

Другое важное направление – повышение безопасности. Причем не только безопасности передачи данных по каналам и обработки в облаке, но и непосредственно на рабочем месте. Интересные решения – экраны со встроенной камерой, отслеживающие положение зрачков пользователя. В резкость попадает только фрагмент экрана, на который обращен взгляд, а остальное изображение размыто. Подход помогает защититься от считывания текста посторонним через плечо в общественном месте, например, в салоне самолета. Ведутся разработки средств защиты от вредоносных программ, регистрирующих различные действия пользователя – нажатие клавиш на клавиатуре, движение и нажатие клавиш мыши, а также делающих снимки экрана или записывающих взаимодействие пользователя с удаленным рабочим столом.

Четко прослеживается тренд интеллектуализации систем безопасности. Так, в контроллерах доставки приложений (шлюзах доступа) анализируется поведение пользователей для выявления ботов, пытающихся получить доступ к системе путем перебора наиболее часто встречающихся паролей с разных IP-адресов. А использование алгоритмов машинного обучения помогает выявлять потенциальных инсайдеров с нетипичным профилем поведения в сети, на которых стоит обратить внимание сотрудникам службы информационной безопасности.



Будущее – за использованием мультиоблачных сред. Пока DaaS объединяет с площадкой заказчика (on-premise) только одного облачного провайдера, но в ближайшее время можно ожидать появления мультиоблачных решений, что позволит пользователю удаленного рабочего стола выбирать наиболее подходящие сервисы у нескольких облачных провайдеров.

Важное направление – уменьшение задержки при передаче сигнала. Мало удовольствия сидеть перед монитором и ждать, когда система отработает посланную команду. Помочь может правильный выбор дата-центра, например, ближайшего к пользователю ЦОДа облачного провайдера или edge-ЦОДа компании, максимально приближенного к месту сбора информации. Среди наиболее экзотичных примеров – использование удаленного рабочего стола облачной платформы GalacticSky, развернутой в космосе на кластере микроспутников, которая разгружает дорогостоящий канал связи с Землей за счет уменьшения количества передаваемых данных.

В ожидании роста рынка

В России сервисы организации удаленного рабочего места предоставляют многие облачные провайдеры.

Например, в облаке #CloudMTS организованы виртуальные рабочие места всего бухгалтерского подразделения российского филиала международной сервисной компании «Европ Ассистанс СНГ». В облако также перенесены сервисы Active Directory, отвечающие за централизованный доступ и аутентификацию пользователей в программах и приложениях. Безопасность удаленного доступа обеспечивается как каналами связи МТС, так и VPN-технологиями.

Сервисы «Ростелекома» для оперативной организации удаленной работы и эффективной коммуникации сотрудников в период неблагоприятной эпидемиологической обстановки в стране задействовала Федеральная пассажирская компания. С помощью комплекса услуг провайдера к внутренним системам ФПК были подключены свыше 3 тыс. сотрудников, работающих вне офиса. Доступ к корпоративным ресурсам осуществляется с применением защищенной удаленной аутентификации, шифрования каналов связи и технологий предотвращения сетевых угроз.

Удаленные рабочие столы в облаке M1Cloud на базе VMware Horizon с возможностью разворачивать от 500 рабочих станций в течение нескольких минут предоставляет крупному бизнесу компания Stack Group.

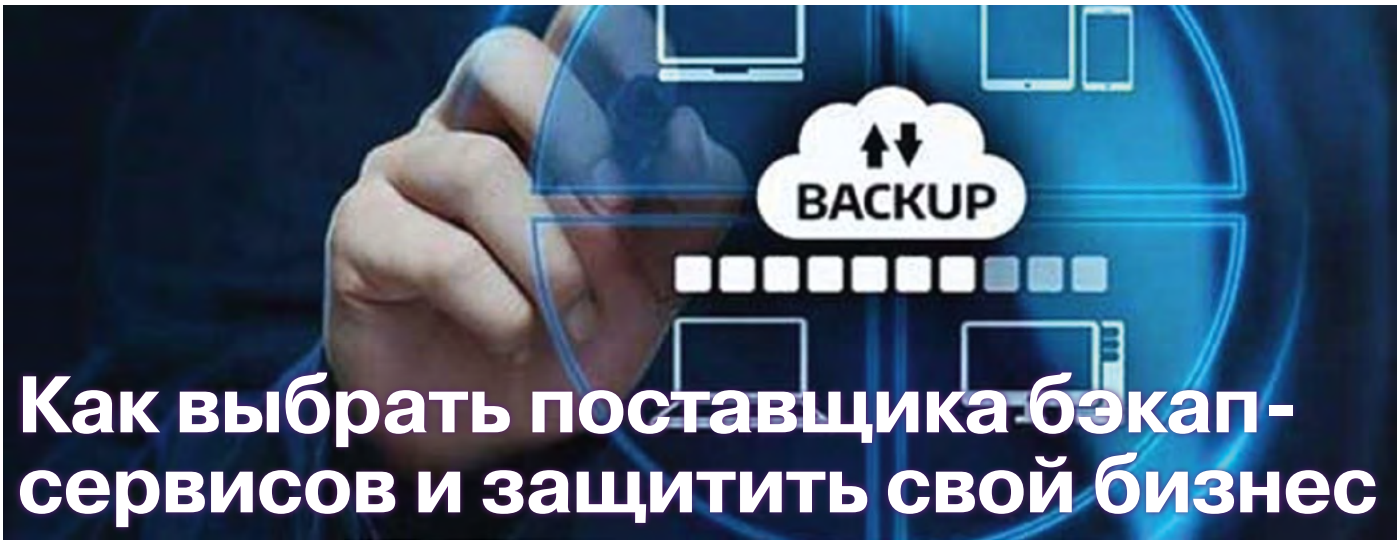
«МегаФон» обеспечивает удаленные рабочие места как для крупного бизнеса (с помощью сервисов VDI), так и для малого и среднего (RDS). Оператор и сам активно использует предлагаемые возможности и в начале периода самоизоляции за несколько дней перевел на удаленную работу более 14 тыс. своих сотрудников.

Тем не менее пока рынок DaaS нельзя назвать оживленным. iKS-Consulting даже не выделяет его в отчетах в отдельный сегмент, объединяя с IaaS. Как комментирует ведущий консультант аналитического подразделения iKS-Consulting Станислав Мирин, в структуре IaaS доля услуги VDI, предоставляемой по сервисной модели из облака (DaaS), сегодня невелика, в доходах облачных провайдеров она составляет менее 2%. Доход от этой услуги обозначили только 20% опрошенных аналитиками провайдеров IaaS. Это говорит о том, что на сегодня DaaS – нишевая услуга. Клиенты чаще всего выбирают между RDS и VDI.

Сравнивая услуги RDS и VDI, эксперт отмечает, что RDS распространена довольно широко и востребована там, где сотрудники используют однотипное ПО и могут работать из разных мест, а не только из офиса. Работодателю эта услуга позволяет сэкономить на использовании тонких клиентов вместо полноценных персональных компьютеров, облегчает администрирование пользователей и обеспечение конфиденциальности данных, с которыми работают сотрудники. Услуга VDI более дорогая, так как требует больше лицензий и ресурсов. Естественно, что облачный провайдер перекладывает эти затраты на заказчика. Услуга обеспечивает пользователю большую гибкость и автономность. Она нужна, например, разработчикам, которые могут в какой-то момент «уронить» операционную систему, но не должны этими действиями мешать другим пользователям.

«По мере проникновения публичных облачных услуг в инфраструктуру компаний сегмент DaaS будет развиваться, но не быстрее облачного рынка в целом», – считает С. Мирин.

Мировой рынок, включающий помимо предоставления непосредственно сервиса техническую поддержку и консалтинг, выглядит более внушительно. По оценкам Future Market Insights, его объем в 2019 г. составил около $3,5 млрд, причем агентство прогнозирует ежегодный 18%-ный рост до 2029 г. Наиболее перспективные сегменты – предприятия малого и среднего бизнеса. Продолжающаяся пандемия подстегнет развитие рынка DaaS. Все больше компаний переходит от работы из офиса к работе с нескольких расположенных в разных местах устройств («удаленка» дома, на даче, в командировке), а DaaS позволяет делать это из любого места и в любое время. ИКС



Как выбрать поставщика бэкап-сервисов и защитить свой бизнес

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

Сегодня услугу резервного копирования предоставляют многие сервис-провайдеры. Каждый – на своих условиях. Как устроен этот рынок и на какие вопросы нужно найти ответы, прежде чем обращаться к провайдеру?

На волне глобальной цифровизации компании осознали: резервные копии данных жизненно необходимы, а затраты на их создание куда меньше тех убытков, которые может понести бизнес в непредвиденной ситуации.

Готовим техзадание

На российском рынке резервное копирование как услугу (Backup as a Service, BaaS) предоставляют многие провайдеры. Это позволяет найти решение практически для любого случая. Прибегая к такой услуге, компании защищают свои данные, соблюдая при этом известное правило «3-2-1» без вложений в удаленную площадку, и переводят расходы на бэкап из CAPEX в OPEX. Кроме того, облачное резервирование данных – шаг в направлении услуги аварийного восстановления из облака (Disaster Recovery as a Service, DRaaS).

При выборе поставщика эксперты советуют компаниям ответить себе на несколько вопросов. Во-первых, составить список систем, данные которых необходимо резервировать. Во-вторых, определить объем резервных копий, которые будут храниться. В-третьих, решить, сколько времени можно выделить на создание резервных копий, как часто их создавать и как быстро нужно восстановить данные в случае повреждения или потери.

На подготовительном этапе заказчик не всегда учитывает перспективы увеличения объема данных, а это влечет за собой дополнительные расходы. У одних провайдеров можно сразу зарезервировать определенный объем, но легко ошибиться в расчетах. У других провайдеров можно ограничить доступный для использования объем, например 1000 Тбайт, и платить только за фактически потребленные ресурсы. В любом случае нужно заранее понимать, сможет ли провайдер обеспечить ваши растущие потребности.

Выбираем поставщика услуги

На рынке работают два типа провайдеров, предоставляющих услугу резервного копирования данных.

Облачные провайдеры. Это классический вариант. Облачные провайдеры оказывают услугу в дополнение к SaaS-, IaaS-, PaaS- и другим видам услуг. Гиганты вроде AWS или Microsoft предлагают резервное копирование в качестве дополнительного сервиса, который резервирует данные, обрабатываемые в их облаках. Отечественные провайдеры (например, «Мегафон Облако», Selectel) на базе одного или нескольких программных продуктов позволяют резервировать как облачные данные, так и те, что хранятся и обрабатываются на площадке заказчика, on-premise.

Производители «железа» и ПО, интеграторы. Этот вариант является гибридом аутсорсинга, аренды (лизинга) и профессиональных сервисов: оборудование системы резервного копирования размещается на площадке заказчика, но не принадлежит ему. Разработка решения, настройка и обслуживание могут выполняться поставщиком услуги или самим заказчиком.

Облачные провайдеры привлекают простотой решения. Как правило, с ними работают компании, имеющие типовую инфраструктуру и стандартное техническое задание. Если же у клиента уникальный софт и есть специфические приложения, то облачные провайдеры их

просто «не потянут» из-за отсутствия или ограниченного выбора нужного ПО. В этом случае лучше обратиться к тем, кто использует проектный подход и готов предоставить сервис BaaS, оптимизированный под заказчика.

Определяем специфику услуги

Большинство сервис-провайдеров проходят сертификацию на соответствие требованиям стандарта PCI DSS (стандарт безопасности данных индустрии платежных карт), GDPR (общеевропейский регламент о защите персональных данных), а также выполняют требования закона 152-ФЗ «О персональных данных».

При планировании резервного копирования и восстановления данных компании важно учитывать допустимые значения параметров RPO (recovery point objective) – максимального периода времени, за который могут быть потеряны данные в результате инцидента, и RTO (recovery time objective) – промежутка времени, в течение которого система может оставаться недоступной в случае аварии. Стандартных значений этих параметров нет. Попробуйте представить, какие убытки понесет, скажем, Ozon или другая крупная онлайновая торговая площадка при простое ИТ-инфраструктуры. Не зная и не понимая этих показателей, заказчик может неправильно оценить риски для бизнеса и составить неверный план восстановления.

Если говорить о самом резервном копировании, то у всех провайдеров данные могут храниться либо в одном, либо в нескольких дата-центрах. Одни предоставляют возможность расширения услуги до DRaaS, другие – нет. Сервис DRaaS позволяет решить возникшие проблемы с инфраструктурой за счет быстрого разворачивания бэкапа в облаке.

Как платить

Оплата услуг резервного копирования может осуществляться ежемесячно, ежемесячно с годовой подпиской, ежемесячно с контрактом на длительный срок или на год вперед. Кроме того, возможна плата за объем, которая может различаться для разных типов клиента или агента, могут также применяться бонусы и неустойки в зависимости от частоты восстановления данных и их объема.

Облачному провайдеру заказчик платит за объем хранения и за типы резервируемых данных и систем. Сама стоимость во многом определяется тем ПО, которое использует провайдер. Такой подход достаточно стандартизирован, автоматизирован и предполагает прозрачную модель оплаты (например, на базе ПО Veeam с открытым прайсом).

Производители «железа», ПО и интеграторы используют проектный подход, при котором можно «бэкапить» сложные системы, применять любое ПО и разрабатывать облако в соответствии с потребностями конкретного заказчика. Стоимость будет зависеть от сложности предлагаемого решения.

Если нет доверия…

Важный вопрос для клиента – защита данных (в том числе от провайдера). Технологически этот вопрос может быть решен путем шифрования данных на стороне заказчика перед отправкой их в облако на хранение без передачи ключей шифрования провайдеру. Однако такой метод доступен не всегда и может значительно увеличить стоимость услуги, например, из-за уменьшения коэффициента дедупликации (отношения объема данных, хранящихся в системе резервного копирования, к размеру образа резервной копии на диске).

Если же вы опасаетесь кибератак и утечек, то гарантией безопасности станут сертификаты соответствия требованиям безопасности информации, которые может предоставить выбранный провайдер. ИКС

МНЕНИЕ ЭКСПЕРТА

Быстрее рынка

Станислав Мирин, ведущий консультант, iKS-Consulting

С развитием цифровой трансформации компаний, для которых данные – неотъемлемая часть производственных и технологических процессов, будет становиться все больше, а объемы данных будут расти по экспоненте. Классический подход к резервированию требует размещения данных на определенном удалении от основного дата-центра, для «горячего» резервирования, как правило, в пределах одного большого города, для «холодного» – лучше в соседнем регионе.

До недавнего времени такую схему могли реализовать только крупные организации, такие как ведущие банки или федеральные ритейлеры. Развитие сетей связи и предложение облачных услуг резервного копирования (BaaS) и аварийного восстановления (DRaaS) позволяет обеспечить сохранность данных более широкому кругу заказчиков. Сервисом резервного копирования в облако дополняют услуги IaaS около 70% их пользователей. Если к услугам DRaaS прибегают в основном крупные компании, то резервное копирование в облако востребовано и у крупных, и у средних компаний. Оказывая услуги BaaS и DRaaS, провайдеры зачастую не ограничиваются предоставлением отдельной виртуальной площадки для хранения резервных копий, а предлагают специализированные решения партнеров для «умного» резервирования, позволяющего экономить место на дисках.

Объем облачных услуг обеспечения сохранности данных растет в России значительно быстрее рынка в целом. Причем сегмент DRaaS, став доступным заказчикам двумя-тремя годами позже, быстро набирает популярность и опережает по темпам роста сегмент BaaS. Мы ожидаем, что в 2021–2024 гг. объем этих услуг в совокупности будет ежегодно увеличиваться не менее чем на 40%.

Взгляд на безопасность КИИ через облака

Мурад Мустафаев, руководитель службы информационной безопасности, «Онланта» (ГК ЛАНИТ)

Для нивелирования рисков, которым подвержены объекты критической информационной инфраструктуры, имеющие облачную компоненту, необходимы системный подход, внедрение решений, поспевающих за развитием угроз безопасности, и совместные усилия субъекта КИИ и облачного провайдера.

Если за системный подход ответственность несет государство, то комплекс мероприятий и непосредственная защита объектов КИИ – задача для организаций-владельцев и облачных провайдеров, которые нередко имеют дело с критическими объектами.

Организация является субъектом КИИ, если одна из составляющих ее деятельности – эксплуатация критически важных систем (объектов КИИ), предназначенных для решения задач государственной обороны, обеспечения правопорядка, управления или безопасности. Функционирование объектов КИИ связано с процессами, нарушение которых может нанести большой ущерб окружающей среде, населению, экономике и административным органам. Эксплуатация таких объектов регламентируется законом 187-ФЗ «О безопасности объектов КИИ в РФ».

Если организация владеет объектом КИИ, на нее автоматически ложится обязанность обеспечивать его безопасность, в том числе информационную, и регулярно доказывать соответствие мер защиты требованиям регуляторов. В некоторых случаях атаки на отдельные объекты могут действовать на всю КИИ по принципу домино. Причем последствия успешных хакерских атак могут быть необратимыми. Вот почему опыт обеспечения информационной безопасности элементов этой экосистемы накапливается централизованно и тщательно систематизируется согласно требованиям регуляторов, а ответственность каждого элемента важна в рамках всей системы. Если организация не уверена в своей способности нести подобную ответственность, ей целесообразно обратиться к внешним подрядчикам, обладающим необходимой экспертизой.

Объект КИИ как предмет аренды

Когда элементом объекта КИИ является арендуемая у провайдера облачная инфраструктура, нужно позаботиться о том, чтобы выстроить в ней систему информационной безопасности. В этом случае задачи защиты облачной части объекта КИИ делятся между компанией-заказчиком и провайдером инфраструктуры. Конечно, с проверкой придут к субъекту КИИ, но сегмент инфраструктуры на стороне провайдера должен быть защищен в соответствии с требованиями ФСТЭК и ФСБ и иметь соответствующий аттестат. Политики безопасности провайдера должны быть подкреплены документами, фиксирующими результаты проведения аудита ИБ сторонней организацией. Однако обязанности провайдера на этом не заканчиваются. Для работы с определенными сегментами КИИ поставщики облачных услуг должны не реже раза в год проводить обучение своих специалистов.

Наличие у провайдера такого фундамента безопасности делает его привлекательным не только для субъектов КИИ, но и для других игроков рынка. Использование аттестованного защищенного облака в комплексе со службой информационной безопасности провайдера позволит им обеспечить безопасность информационной системы с нуля без лишних финансовых, временны́х и организационных затрат, а также дополнительных рисков из-за отсутствия опыта. Встраивание же функций и инструментов безопасности в системы, сети и оборудование уже после их ввода в эксплуатацию сопряжено с рядом рисков, самый серьезный из которых – необходимость отключать системы для установки обновлений.

Дополнительным драйвером для отечественного рынка стала инициатива Министерства цифрового развития, связи и массовых коммуникаций РФ в сжатые сроки «переодеть» КИИ в отечественные решения – перевести все объекты на преимущественное использование российского ПО (до 1 января 2021 г.) и оборудования (до 1 января 2022 г.). Такая инициатива замыкает выбор поставщиков облачных решений на тех, которые могут гарантировать полную локализацию своих продуктов в России.

Как разделить объекты по уровню критичности и оценить риски ИБ

Чтобы грамотно выстроить приоритеты в системе информационной безопасности объектов КИИ, необходимо сначала провести инвентаризацию активов (эту процедуру полезно совместить с категорированием объектов КИИ – одним из этапов обеспечения их защиты). Для категорирования формируется команда из специалистов по разным направлениям. Коллегиально они выявляют критические процессы и активы, собирают объекты КИИ, которые подлежат категорированию, определяют угрозы безопасности, категории значимости объектов и т.д. При предварительной оценке объектов есть вероятность ошибиться с категорией. Поэтому важно грамотно подобрать состав команды или доверить категорирование объектов профильным организациям.

Объекты КИИ оцениваются, исходя из их социальной, политической, экологической и экономической значимости, а также значимости для обороны страны, безопасности и охраны правопорядка. От этой оценки зависит, будет ли объекту присвоена какая-либо из трех категорий значимости или он будет признан незначимым. От уровня значимости объекта КИИ зависит набор организационных и технических мер, обеспечивающих нейтрализацию угроз, последствиями которых может быть прекращение или

нарушение его работы. К незначимым объектам КИИ требования ниже. Для информационных систем, осуществляющих обработку персональных данных, определяется также уровень защищенности в зависимости от типов угроз, данных, обрабатываемых системой, и ее пользователей.

После инвентаризации становится ясен вектор работ по выстраиванию системы информационной безопасности. Критичность актива отражает степень влияния его функционирования на бизнес-процессы организации с точки зрения безопасности, отказоустойчивости и эффективности. После анализа критичности следует выработать план непрерывности бизнеса (Business Continuity Plan, BCP) и план послеаварийного восстановления инфраструктуры (Disaster Recovery Plan, DRP). В разработке этих планов участвуют все, кто взаимодействует с объектами КИИ. То есть если инфраструктура находится на стороне провайдера, он должен принимать непосредственное участие в распределении активов по уровню критичности и планировании непрерывности работы систем. Отказоустойчивость инфраструктуры – ключевой элемент договора с провайдером, который закрепляется в соглашении об уровне оказания услуги. Надежные провайдеры гарантируют отказоустойчивость на уровне трех элементов: гипервизор, сеть и системы хранения данных.

Детально разработанные планы BCP и DRP будут дорожной картой спасения активов в случае возникновения инцидентов. Сценарии из этих документов нужно регулярно тестировать и корректировать, так как субъектам КИИ установлены строгие временны́е рамки для сообщения об инциденте в Национальный координационный центр по компьютерным инцидентам. А субъектам банковского сектора необходимо уложиться в три часа с момента обнаружения инцидента, чтобы проинформировать еще и Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере.

При анализе потенциальных рисков информационной безопасности на объекте КИИ лучший вариант – организовать проверку «на 360 градусов». Как это сделать? Во-первых, провести аудит ИБ для обнаружения слабых мест в системе защиты инфраструктуры. Во-вторых, смоделировать атаку на целевую систему, чтобы оценить ее готовность встречать реальные атаки. Второе предполагает привлечение сторонних специалистов («белых хакеров») для проведения тестирования на проникновение. К такого рода проверке не стоит относиться скептически, она дает ценные результаты. А для защиты конфиденциальных данных целесообразно подписать с провайдером соглашение о неразглашении.

Изучив объект КИИ «насквозь», можно максимально прозрачно оценить все факторы, определяющие риски наступления неблагоприятных событий ИБ, увидеть слабые стороны, «дыры», лазейки, оценить ущерб до его наступления и вовремя подготовиться. Информационная безопасность КИИ не должна ограничиваться защитой на стороне субъекта КИИ, порой некоторые обязательства распространяются даже на контрагентов. При этом опытные облачные провайдеры уже обладают экспертизой, накопленной в результате реагирования на различные инциденты ИБ.

Угрозы ИБ в облаках

Злоумышленники все чаще выбирают мишенью для своих атак наименее защищенные элементы в ИТ-инфраструктуре, к которым относятся в том числе публичные облака. Одна из частых причин – неправильная конфигурация облачных платформ. Известны случаи, когда хакеры через облачные сервисы получали доступ к корпоративной инфраструктуре для поиска конфиденциальной информации, пригодной для продажи, или перенаправления зарплат и платежей на свои счета. Взломщики без труда обходили двухфакторную аутентификацию и через незащищенный протокол IMAP похищали аккаунты руководителей и административного персонала.

Одним из элементов инфраструктуры провайдера является гипервизор, который «нарезает» облако на виртуальные машины. Атака на гипервизор может привести к перехвату одной виртуальной машиной ресурсов и информации, доступных другой машине. Используя уязвимости гипервизора, можно нарушить работу всего облака и получить несанкционированный доступ к образам виртуальных машин вплоть до захвата всей инфраструктуры. Безопасный гипервизор должен уметь идентифицировать и контролировать доступ пользователей к виртуальным машинам, ограничивать права эмуляторов устройств до минимально необходимых, выявлять атаки и контролировать сетевые взаимодействия. Если провайдер облака не располагает таким решением, то гипервизор становится потенциальным источником серьезных рисков.

Принцип работы облачных сервисов (доступ из любого места в любое время) предполагает децентрализацию информации и устройств, имеющих к ней доступ. Если злоумышленнику удастся скопировать токен аутентификации, он сможет удаленно проникнуть в защищенный контур облачной инфраструктуры. Получить токены можно методами социальной инженерии. Такие атаки появились не так давно и получили название «человек в облаке».

Уязвимым звеном облачной модели является внешняя веб-среда. Передача данных и запросы к информационной системе в облаке провайдера должны идти через изолированные зашифрованные туннели. Поскольку большинство пользователей облачных систем подключаются к облаку через браузер, реализуются такие угрозы, как межсайтовый скриптинг, кража паролей, перехваты веб-сессий, компрометация каналов связи с искажением передаваемой информации.

Один из наиболее значимых факторов, останавливающих потенциальных заказчиков облачных сервисов, – DDoS-атаки, способные вывести из строя сегмент облака. При такой атаке множеством распределенных запросов к системе создается большая нагрузка на целевую инфраструктуру, которая доводит ее до отказа в обслуживании и делает ресурсы на некоторое время недоступными. Однако облака на то и облака, что при росте нагрузки на систему можно оперативно увеличить ее мощность, чтобы восполнить недостающие ресурсы. Дополнительной возможностью, предоставляемой провайдером, является резервирование данных, а иногда и рабочих процессов, на отдельной инфраструктуре. В таком случае при остановке основного ЦОДа можно быстро переключиться на работу в резервном, не теряя непрерывности процессов.

Облачные средства защиты объектов КИИ от угроз ИБ

Результатом качественного анализа безопасности критической инфраструктуры должна быть дорожная карта с комплексом мер, необходимых для проектирования эффективной системы ИБ на объекте. В случае сотрудничества с облачным провайдером защитой объекта занимается помимо самой организации еще и поставщик услуг, что дает синергический эффект. Облачный провайдер должен иметь не только расширенный актуальный аппаратно-программный комплекс защиты информации, но и штатных специалистов по информационной безопасности для мониторинга объектов КИИ, размещенных в облаке, и грамотной модернизации системы ИБ всей инфраструктуры.

Минимальная планка мер по защите инфраструктуры на стороне провайдера облачных решений – соответствие требованиям регуляторов. Но хороший подрядчик этим не ограничивается.

Для облачной защиты от внешних атак зачастую используются межсетевые экраны, фильтрующие веб-трафик в соответствии с заданными правилами. Комплексы WAF (Web application firewall) контролируют трафик, проходящий через веб-приложения в облаке, осуществляют сигнатурный и поведенческий анализ, сканирование уязвимостей, виртуальный патчинг. Кроме прочего, в облаке устанавливаются системы обнаружения и предотвращения вторжений (IPS/IDS), неочевидными функциями которых являются поиск открытых незащищенных портов и вредоносных программ, проникающих через них, а также попыток неавторизованного доступа. Эти системы помогают оценить уровень критичности обнаруженных угроз, что немаловажно для проектирования защиты объекта КИИ.

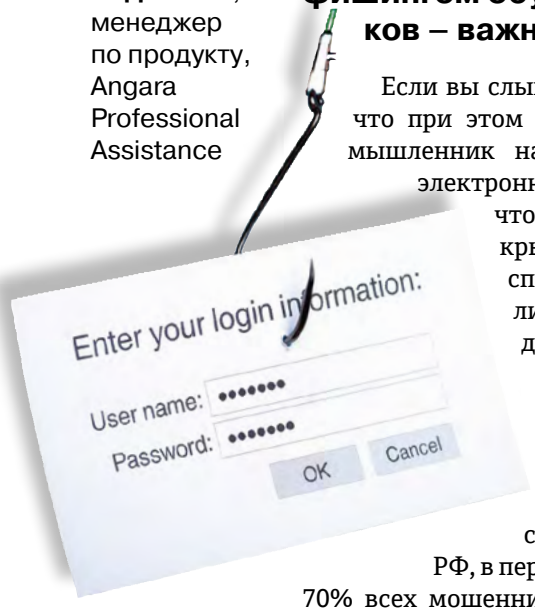
Некоторые провайдеры идут дальше и выстраивают единую систему управления угрозами, объединяющую функции антивируса, систем обнаружения и предотвращения вторжений, пакетного фильтра и VPN-шлюза в одной программе. Хорошим инструментом также является система SIEM (Security Information and Event Management). Она консолидирует и анализирует информацию со всех сетевых устройств и систем безопасности, предупреждает об аномальных событиях и фиксирует логи для последующего обучения. Это решение использует технологии искусственного интеллекта, и оно довольно дорогое, не каждой организации по карману. Мало просто приобрести такую систему, в штате должны быть высококвалифицированные специалисты, которые сумеют тонко настроить ее для эффективной эксплуатации. В противном случае деньги будут потрачены зря. Облачные провайдеры, обладающие продвинутым центром мониторинга и реагирования на инциденты ИБ, и дистрибьюторы услуг информационной безопасности имеют возможности и резоны использовать SIEM-системы не только в своих интересах, но и на благо заказчиков.

Все вышеперечисленные инструменты, конечно, полезны, но говоря о защите КИИ, нельзя обойти вниманием организационные меры. Эффект от внедрения самых продвинутых инструментов окажется нулевым, если сотрудники не будут соблюдать правил корпоративной «кибергигиены» – будь их действия беспечными или злонамеренными, подрывающими безопасность объекта КИИ. Любые WAF и SIEM бессильны в ситуации, когда сотрудник подключает к изолированной сети флеш-носитель, который может содержать скрытый вредоносный код, способный «обрушить» весь объект или целый сегмент КИИ. Соответствующие требования должны быть детально прописаны в пакете организационно-распорядительной документации. Не проверяя сотрудников на предмет соблюдения требований ИБ и не регламентируя их действия, организация ставит крест на безопасности объекта КИИ и на своей ответственности как игрока рынка. ИКС

Предупрежден – значит вооружен

Яна Анджелло, менеджер по продукту, Angara Professional Assistance

Как и во многих вопросах информационной безопасности, в борьбе с фишингом обучение и повышение уровня осведомленности сотрудников – важное звено системы защиты бизнеса.



Если вы слышали о фишинге, то знаете, что при этом типе мошенничества злоумышленник направляет вам фальшивое электронное письмо или сообщение, чтобы обманом побудить раскрыть важные данные (паспортные, платежные, пароли) для последующей кражи денежных средств.

Большинство из нас уверены, что никогда не попадутся на такую махинацию. Однако статистика говорит об обратном. Согласно сведениям Генпрокуратуры РФ, в первом полугодии 2020 г. почти 70% всех мошенничеств пришлись на обманные схемы с использованием интернета и мобильных средств связи. Большие объемы личной информации в открытом доступе, развитие и доступность новых технологий, эффективность и дешевизна такого вида атак – и фишинг сегодня представляет бóльшую угрозу, чем когда-либо. Ваш бизнес и ваши сотрудники в любой момент могут оказаться в опасности.

История

Впервые слово «фишинг» было использовано в январе 1996 г. группой хакеров, которые крали учетные записи и пароли America Online. Термин также был использован в журнале The Hacker Quarterly. По аналогии со спортивной рыбалкой интернет-мошенники пользовались приманкой, только электронной, устанавливая «крючки» для выуживания паролей и финансовых данных в море интернета, где плавали пользователи. И если в начале пользователей было не так много, то в течение следующего десятилетия с ростом популярности Глобальной сети и электронной почты у киберпреступников появились уже миллионы ничего не подозревающих жертв. Еще шире распространился фишинг в 2007 г., когда на рынке появились смартфоны и пользователи получили постоянный доступ к e-mail.

Сегодня фишинг затрагивает не только электронную почту. Благодаря современным технологиям атаки приобретают разнообразные формы и осуществляются по разным каналам. В арсенале киберпреступников – SMS (смсинг), телефонные звонки (вишинг), мессенджеры, социальные сети, поддельные домены, а также инструменты для имитации голоса и другой биометрии. Например, в 2019 г. впервые был использован голосовой дипфейк (подделка голоса). В компанию, ставшую жертвой мошенничества, позвонил якобы генеральный директор и дал указание сотрудникам срочно перевести 220 тыс. евро на указанный счет, что и было сделано.

Тренды

Большинство из нас знает, что нигерийским «принцам» доверять нельзя, но сочетание технологий и социальной инженерии породило фишинговые атаки, способные ввести в заблуждение даже сотрудника отдела безопасности. Обман строится на доверии пользователя, и главная задача преступника заключается в качественной имитации привычных жертве процессов: покупки товара или услуги, решения рабочих задач, выстраивания коммуникаций.

Появление социальных сетей существенно облегчило злоумышленникам поиск личной информации о потенциальной жертве, ее предпочтениях и слабых местах, на которой и выстраивается «легенда» обмана. Благодаря нехитрой процедуре сбора «цифрового анамнеза» мошенники создают персонализированную схему обмана, которая не вызовет ни малейшего подозрения. Злоумышленники могут подделывать стиль деловой переписки, манипулировать информацией о семейном положении и т.д. Многие отправители фишинговых писем искусно выдают себя за доверенное лицо или компанию. Так, во время отчетного периода мошеннические сообщения могут быть похожи на сообщения от Федеральной налоговой службы России.

Киберпреступники начали персонифицировать атаки. Теперь перед тем, как провести атаку, они просят жертву заполнить несложную

форму или документ и только после этого отправляют пользователя на фишинговый сайт. Зачастую такая активность кажется легитимной, что затрудняет ее обнаружение.

Злоумышленники научились маскировать поддельные веб-ресурсы фирменным стилем и аутентичной информацией, полученной из известных и надежных источников. Поэтому зачастую фишинговый сайт практически невозможно отличить от оригинального. Причем копированию подвергаются веб-ресурсы крупных и надежных компаний, например РЖД. Кроме того, согласно статистике PhishLabs, 58% всех фишинговых сайтов используют HTTPS, что снижает вероятность идентификации веб-сайта в качестве мошеннического, поскольку браузеры отмечают соединение как защищенное. Эта тактика стала эффективной мерой усыпления бдительности пользователя.

Независимо от того, насколько защищен ИБ-периметр организации технически, защитить его от людей невозможно. Для бизнеса сотрудники – весомый фактор риска, даже если они этого не хотят. Об этом говорят многочисленные исследования:

- 32% подтвержденных утечек информации связаны с фишингом (по данным отчета 2020 Data Breach Investigation Report, подготовленного оператором Verizon);
- каждое 25-е письмо в деловой переписке – фишинговое (согласно оценкам компании Avanan);
- 90% фишинговых атак проходят через защищенные почтовые шлюзы (по данным компании TrendMicro);
- 37,9% пользователей не сдают учебные тесты на противодействие фишинговым атакам (информация из отчета 2020 Phishing By Industry Benchmarking компании KnowBe4).

Преступники знают об этом и будут продолжать эксплуатировать неосведомленность сотрудников, используя фишинговые атаки и социальную инженерию.

Что делать?

В первую очередь бизнесу необходимо осознать и признать опасность социальной инженерии и человеческого фактора. После чего нужно спланировать комплекс мероприятий и выделить ресурсы для повышения осведомленности персонала.

Обучение сотрудников. Образованный сотрудник – надежная защита от фишинговых атак. Даже если у компании установлена лучшая в мире система обнаружения спама, фишинговые письма все равно пройдут. Кроме того, сотрудник может поставить под угрозу бизнес, если он станет жертвой телефонного мошенничества, использует зараженное устройство на работе или по неосторожности оставит свои данные на фишинговом сайте.

Инвестируйте время и ресурсы, чтобы обучать свой персонал не только распознавать фишинг, но и иметь представление о «компьютерной гигиене» в целом. Таким образом он сможет адекватно реагировать на угрозы и мошенничество, сохраняя ваш бизнес в безопасности.

Многие ИБ-компании предлагают курсы по антифишингу, и некоторые из них можно пройти бесплатно в варианте «промо». Помимо этого, компания может самостоятельно сформировать свод базовых правил и знакомить с ним новых сотрудников.

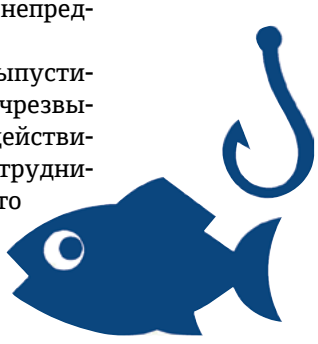
Тестовые атаки. Когда дело доходит до фишинга, опыт – лучший учитель. Если вы не хотите стать жертвой настоящей фишинговой атаки только для того, чтобы узнать, как она выглядит, то стоит провести тестовые атаки. Современные методы обучения включают в себя имитацию фишинговых атак.

Сейчас можно фишить своих сотрудников (конечно, не крадя их информацию) с помощью специализированных сервисов или решений. Хотя это может показаться бесчестным, имитация фишинговых атак – весьма эффективный способ дать сотрудникам практический опыт в выявлении и реагировании на мошенничество. В среднем нарушение конфиденциальности данных обходится малому бизнесу в $3 тыс. (или больше), поэтому имитация фишинговой атаки может быть ценной инвестицией, которая сэкономит деньги компании в долгосрочной перспективе.

Политика безопасности. Убедитесь, что в вашей компании реально действует хотя бы базовая политика безопасности. Установите принципы поведения сотрудников на рабочем месте и рядом с ним. Как допускается использовать корпоративные компьютеры? Запрещены ли какие-либо программные приложения или вебсайты? Разрешено ли сотрудникам приносить с собой свои личные устройства?

Подумайте о том, кто и к каким типам информации имеет доступ, ограничьте доступ к конфиденциальным данным. Это поможет контролировать и защищать информацию от непреднамеренного разглашения или кражи.

Наконец то, о чем многие забывают: выпустите рекомендации, что делать в случае чрезвычайной ситуации. Если ваш бизнес действительно стал жертвой кибератаки, то сотрудники должны знать, как реагировать. Это поможет устранить проблему и минимизировать ущерб. Не забывайте о главном правиле – предупрежден, значит вооружен. ИКС



«Болезнь легионеров»: скрытая опасность для крупных ЦОДов

Олег Котелюх, управляющий партнер, «Инпро Технолоджис»

На фоне COVID-19 перед дата-центрами остро, как никогда раньше, встал вопрос о защите сотрудников от легионеллеза, «болезни легионеров». Почему именно ЦОДы первыми оказались под ударом и как они могут победить вездесущую инфекцию?

В то время как офисы были закрыты во время вспышки коронавируса, ЦОДы работали с повышенной нагрузкой. С первых же дней кризиса индустрия ЦОДов поддерживала массированный переход на удаленный режим работы, а также более широкое использование онлайн-сервисов и цифровых коммуникаций. Как следствие, нагрузка на дата-центры выросла в разы, из-за чего им пришлось увеличить мощность систем охлаждения.

В итоге руководители ЦОДов были вынуждены решать проблемы, которые долгие годы оставались «за кадром»: когда градирни заработали в полную силу, стало очевидно, что коррозия труб и застой воды в них могли привести к росту бактерии легионеллы. И как только капли воды с этой бактерией начали попадать в атмосферу, это повысило риск вспышки легионеллеза – заболевания, поражающего легкие пациента и приводящего к смерти в каждом десятом случае.

При чем тут легионеры?

Первое упоминание о легионеллезе связано со вспышкой респираторного заболевания в 1976 г., когда после одной из встреч Американского легиона (организации ветеранов боевых действий) 221 человек заболел неизвестной формой пневмонии. Более тридцати из них скончались. Источник заражения – бактерию *Legionella* вида *L. pneumophila* – обнаружили в гостиничной системе кондиционирования. Оказалось, что легионеллы, обычно безвредные в природе, становятся смертельно опасными для здоровья человека, когда растут в плохо обслуживаемых системах водоснабжения, отопления или вентиляции.

С тех пор общим термином «легионеллез» стали описывать несколько форм инфекции, вызываемой легионеллой. При нелегочной форме, или «болезни Понтиака», пациенты с симптомами, похожими на сезонный грипп, выздоравливают за три-пять дней даже без медицинского вмешательства. Куда серьезнее обстоит дело с «болезнью легионеров». Это тяжелая легочная инфекция, которая может привести к летальному исходу из-за прогрессирующей пневмонии с дыхательной недостаточностью.

Болезнь легионеров, как правило, протекает с выраженной лихорадкой, потерей аппетита, вялостью, а также поражением легких и центральной нервной системы. Почти у половины пациентов развиваются гнойная мокрота или кашель с кровью. Такое состояние требует лечения антибиотиками, нередко – наблюдения за пациентом в стационаре. И даже при таком подходе каждый десятый случай оканчивается смертью.

Источники легионеллеза

В 2018 г., по данным Европейского центра профилактики и контроля заболеваний, в Европе было зарегистрировано 11 343 пациента с диагнозом «легионеллез». Еще около 6 тыс. случаев ежегодно фиксируют в США. И цифры только увеличиваются: несмотря на улучшение тестов на легионеллы, отчеты Центра по контролю за заболеваниями США показывают рост числа заболевших на 550% с 2000 г.

Во многом это обусловлено тем, что источником легионеллы может стать любая застойная некипяченая вода в водонагревателях, систе-

мах отопления или кондиционирования воздуха. Микроорганизм обитает во влажной среде при температурах от +15 до +50°С, а в человеческий организм попадает воздушным путем вместе с водяными брызгами, туманом, конденсатом. Например, бактерии легионеллы, собирающиеся в увлажняющих камерах централизованных систем кондиционирования, могут распространиться по всему зданию.

И все же основным источником болезнетворных организмов были и остаются плохо обслуживаемые градирни и холодильные установки дата-центров, действующие по принципу испарительного охлаждения. Градирни в процессе работы выбрасывают воздух, содержащий капли воды, температура которых идеально подходит для размножения бактерий. С водяными парами в атмосферу отводится более 90% тепла от охлаждаемого оборудования. А вместе с ним и *Legionella*.

Недавно ЦКЗ США подсчитал, что 27% градирен загрязнены этой бактерией. Капли, содержащие микроорганизмы, могут разлететься на расстояние до 10 км от установок. Так, летом 2015 г. в Южном Бронксе от вспышки болезни легионеров, начавшейся предположительно от зараженных легионеллой градирен, пострадали около 140 и погибли 16 человек.

Как дата-центры сражаются с легионеллезом

В первую очередь от заражения легионеллой страдают крупные ЦОДы, которые используют для охлаждения миллионы литров воды ежегодно. Нужно понимать, что традиционные методы очистки, такие как дезинфекция воды хлором в одобренных СанПиН количествах, в случае с легионеллой неэффективны. Бактерия устойчива к хлорсодержащим веществам.

Какие меры профилактики могут предпринять дата-центры, столкнувшиеся с угрозой?

Мгновенная температурная обработка. Бактерии легионеллы не могут размножаться уже при 55°С, а воздействие температуры 70–80°С для них губительно. Вместе с добавлением ультрафиолета или биоцидов (химических средств, предназначенных для борьбы с болезнетворными микроорганизмами) этот простой метод дает хорошие результаты.

Умягчение воды катионитом. Накипь, образовавшаяся из-за жесткой воды, приводит к увеличению шероховатости внутренней поверхности труб и стимулирует рост органических отложений. В этих отложениях формируются продукты коррозии и обитают другие микроорганизмы, обеспечивающие благоприятную среду для легионеллы. Поэтому в ЦОДе нужно умягчать воду, например, путем ее фильтрования через слой катионита, содержащего катионы натрия. Такой метод позволяет снизить показатель общей жесткости воды до менее чем 0,3 мг/л и полностью избежать накипи.

Электрохимическая обработка воды. Окислительно-восстановительные реакции, происходящие в результате пропускания через воду постоянного электрического тока, помогают очистить ее от тяжелых металлов, хлора, фтора и их производных. Реализация этого подхода в одном голландском дата-центре позволила подавить процесс коррозии и избавиться от 600 л химикатов, которые компания использовала для очистки воды ежегодно.

Переход на непосредственное, или погружное, жидкостное охлаждение. Охлаждать стойки дата-центра можно не только воздухом или водой. В последнее время на рынке все шире распространяется идея использования системы непосредственного жидкостного охлаждения, когда вычислительное оборудование погружается в специальные диэлектрические жидкости. Они не проводят ток, не агрессивны к покрытиям и, что важно, не являются питательной средой для микроорганизмов. В итоге снижаются не только риск легионеллеза, но и энергозатраты на нормальное функционирование ЦОДа.

Безопасности ради

Конечно, создание полноценного контура защиты от легионеллы стоит дорого и страх перед финансовым ударом заставляет некоторых менеджеров отрицать саму идею возможности эпидемии. Тем временем риск вспышки легионеллеза с каждым днем повышается. Поэтому дата-центрам необходимо до выхода удаленно работающих сотрудников пересмотреть текущую политику в области «гигиены» градирен. Они могут разработать собственные меры поддержания чистоты систем охлаждения или же (для начала) воспользоваться следующими советами:

- обеспечить поступление в воду химикатов в необходимых количествах, составить график мониторинга этого процесса и назначить ответственное лицо;
- продолжать циркуляцию очищенной воды внутри охладительной системы не менее часа в неделю;
- убедиться, что водохранилища продезинфицированы.

Методы диагностики легионеллеза, хоть и шагнувшие вперед в последние годы, в целом недостаточно быстры, чтобы предупредить потенциальные вспышки заболевания. А на руководителях дата-центров по-прежнему лежит серьезная ответственность за здоровье и безопасность сотрудников. И это именно тот случай, когда «лучше перебдеть, чем недобдеть». ИКС

Система мониторинга параметров окружающей среды и доступа в стойки

Компания Schneider Electric представила пополнение своей системы мониторинга параметров окружающей среды и/или обеспечения безопасности стойки, помещения или зоны в вычислительном центре – миниатюрную систему NetBotz 755.

Система укомплектована светочувствительной видеокамерой Camera Pod 165 (NBPD0165) с частотой съемки 30 кадров/с. Камера обеспечивает обнаружение и запись движущегося объекта, что позволяет сопоставить видеозапись с фактом доступа или сигналом проникновения в охраняемую среду, и поддерживает новый формат высокого разрешения. Также к системе можно подключить до трех внешних камер.

Поддерживаются следующие универсальные датчики APC: 0–5 В, датчик открывания двери, беспотенциального контакта, точечной утечки жидкости, влажности, задымления, температуры, вибрации. У системы четыре порта универсальных датчиков, кроме того, она способна управлять 47 беспроводными датчиками температуры и датчиками температуры/влажности в едином интерфейсе NetBotz.

Контроллер доступа к стойкам NBPD0175 для работы с электронными замками (NBHN125, NBHN1356) обеспечивает ведение журнала с записями о тех, кто получал доступ к шкафам, чтобы организация могла соблюдать требования к безопасности данных. Авторизованным пользователям доступ к оборудованию может предоставляться с помощью бесконтактных карт.

Интеграция со стойками APC, датчиками NetBotz и системой Data Center Expert упрощает развертывание, конфигурирование и управление. NetBotz 755 также может работать под «зонтиком» системы EcoStruxure IT Expert.

Тип сети обмена данными – 10/100/1000BASE-T. Габариты устройства – 14,0 x 24,4 x 9,1 см (В x Ш x Г), вес – 1,56 кг. Рабочая температура окружающей среды – 0...45 °С.

Возможные варианты поставки:

- NBWL0755 – устройство без источника питания, поддерживает питание по Ethernet PoE v.2;
- NBWL0756 – комплект NetBotz Room Monitor 755 + инжектор питания 100–240 В – PoE v.2.

www.schneider-electric.ru

Российские SSD-накопители в формфакторе U.2

Компания GS Nanotech разработала и запустила в производство твердотельные накопители в формфакторе U.2 с интерфейсом PCIe NVMe. Модель предназначена для построения высокопроизводительных систем хранения данных на основе all flash-решений.

Технические характеристики GS SSD U.2:

- объем памяти – 1 Тбайт, 2 Тбайт;
- тип NAND флеш-памяти – 3D TLC;
- интерфейс – PCIe Gen3x4 NVMe;
- максимальная скорость последовательной записи – до 1000 Мбайт/с;
- максимальная скорость последовательного чтения – до 3200 Мбайт/с;
- максимальная скорость произвольного чтения – до 460 000 IOPS;
- максимальная скорость произвольной записи – до 70 000 IOPS;
- ресурс – 0,7 цикла перезаписи полного объема накопителя в день;
- диапазон рабочих температур (в зависимости от варианта исполнения) – стандартный 0...+70˚С или расширенный –40...+85˚С;
- корпус – алюминий.

GS SSD U.2 – это первый твердотельный накопитель в формфакторе U.2, полностью разработанный в нашей стране и произведенный на основе NAND-памяти, корпусированной в России. Весь производственный цикл – разработка и проектирование SSD, корпусирование модулей NAND-памяти, монтаж компонентов на плате, финальная сборка и упаковка изделий — выполняется в кластере «Технополис GS» в Калининградской области.

Линейка твердотельных накопителей GS Nanotech также включает модели в формфакторах 2,5” и M.2 с интерфейсами SATA и PCIe, имеющие емкость до 2 Тбайт. Несколько моделей уже получили заключение Минпромторга о подтверждении производства на территории РФ.

www.gsnanotech.ru

Высокоскоростной шифратор Ethernet

Российская компания «СИС крипто» пополнила свою линейку высокоскоростных шифраторов (ВСШ) каналов распределенных сетей Ethernet L2 «Палиндром», выпустив «Палиндром-6140» — шифратор корпоративного и операторского класса.

Устройство предназначено для шифрования опорных сетей между ЦОДами и других применений с высокими требованиями к пропускной способности. Обеспечивает полнодуплексное шифрование на скорости до 10 Гбит/с без потерь кадров, с накладными расходами пропускной способности не более 8 байт на кадр и типичной вносимой задержкой меньше 10 мкс.

ВСШ построен на специализированной платформе шифрования с ПЛИС. В криптомодуле реализован блочный шифр ГОСТ 34.12-2015 «Кузнечик» (ожидается получение сертификата ФСБ России на СКЗИ по классу КС3). У модели дублированные блоки питания и вентиляторы. Корпус защищен от зондирования (физического взлома без открывания корпуса), а в случае вскрытия корпуса шифратор останавливается и вся ключевая информация стирается.

Поддерживаются линейный («точка – точка») и многоточечный (причем с отдельными туннелями для разных VLAN) режимы соединения между шифраторами. Защищенный канал можно проложить через разные виды физического транспорта Ethernet («темное» оптоволокно, сети OTN, Ethernet с коммутацией на L2, псевдопровода через MPLS и IP). С точки зрения интеграции в сеть ВСШ полностью реализует принцип «узел на проводе»: он совместим с кадрами Ethernet любых форматов (в том числе Q-in-Q и MAC-in-MAC), не вмешивается в работу протоколов слоя контроля L2 и выше. Полноценно реализованы мутация (временная подмена) EtherType, отступ шифрования перед заголовками и пропуск незашифрованных кадров с особыми MAC-адресами, EtherType и VLAN. Для использования по модели управляемого сервиса шифраторы поддерживают мультитенантность с взаимной криптографической изоляцией трафика разных абонентов.

Для администрирования используются интерфейс командной строки (через последовательный консольный порт) и фирменная система управления (станция с ОС Windows, работающая через сеть во внеполосном или внутриполосном режиме). Отдельного контрольного сервера нет, и после отключения станции управления защищенная сеть может работать автономно. Централизованное распоряжение ключами реализовано с помощью сертификатов, выданных сторонними удостоверяющими центрами. Администрирование включает в себя в основном настройки, связанные с криптографией, туннелями и политиками обработки кадров в зависимости от их содержимого, при этом сами туннели устанавливаются автоматически (в том числе в многоточечном режиме).

www.ciscrypto.ru

Огнестойкая СКС

Компания ДКС вывела на рынок огнестойкую СКС, построенную на основе огнестойких кабелей «витая пара» от категории 5е до категории 7А.

Предлагаемые в составе СКС кабели FRHF, согласно ГОСТ МЭК 60331-23, в условиях пожара сохраняют работоспособность в течение 180 мин, обеспечивая при этом гарантированную скорость передачи данных от 100 Мбит/с и выше.

Основная область применения продукта – инженерные и технологические системы, системы критической инфраструктуры, которые должны продолжать работать в условиях пожара и выполнять свои функции как можно дольше. Другой отраслью, для которой ДКС предлагает свои огнестойкие СКС, являются ЦОДы.

Огнестойкая СКС от ДКС включает в себя полный набор медных компонентов: кабели «витая пара» в исполнении нг(А)-FRHF класса пожарной опасности П1б.1.1.2.1, коммутационные панели, розеточные модули keystone и коммутационные шнуры в экранированном и неэкранированном вариантах.

www.dkc.ru

РЕКЛАМА В НОМЕРЕ

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.

АНАЛИТИЧЕСКИЙ ОТЧЕТ

«Российский рынок коммерческих дата-центров 2020»

iKS CONSULTING

Предварительная структура отчета*

Введение	
Цель исследования	
Методика проведения исследования	
1. Текущее состояние рынка кЦОДов в России и в мире	1.1. Стойки: динамика, структура качества, загрузка • Рост числа стойко-мест • Прирост совокупной емкости • Прогноз числа коммерческих стоек • Динамика сегмента Tier III • Утилизация 1.2. Доходы: темпы развития, структура по направлениям • Динамика рынка • Структура доходов ЦОДов по видам услуг 1.3. Потребители • Средний чек и структура клиентов по размеру компаний • Отраслевая сегментация потребителей • Региональная структура выручки коммерческих дата-центров • Структура выручки по типу собственников бизнеса клиентов 1.4. Структура затрат кЦОДов 1.5. Россия на фоне международного рынка услуг ЦОДов
2. Лидеры рынка кЦОДов	2.1. Рейтинг по числу стоек 2.2. Рейтинг по доходам в сегментах Colocation/Cloud/Telecom
3. Структура рынка по игрокам	3.1. Отраслевая структура рынка по игрокам 3.2. Региональная структура 3.3. Операторские дата-центры на рынке коммерческих ЦОДов
4. Региональные сегменты рынка кЦОДов	4.1. Москва и Московская область 4.2. Санкт-Петербург и Ленинградская область 4.3. Региональные коммерческие ЦОДы 4.4. География и связность коммерческих ЦОДов 4.5. Доступ к энергетике для ЦОДов в регионах России
5. Тенденции развития рынка дата-центров в 2019–2020 гг.	5.1. Коронавирус и экономический кризис: последствия для отрасли 5.2. Цифровая трансформация 5.3. Меры государственной поддержки отрасли ЦОДов 5.4. Облачные услуги в бизнесе кЦОДов 5.5. Модели партнерства на рынке кЦОДов
6. Прогноз и перспективы развития рынка ЦОДов в 2020–2023 гг.	6.1. Основные драйверы и процессы, замедляющие развитие рынка кЦОДов в России 6.2. Коммерческие ЦОДы и национальная программа «Цифровая экономика» 6.3. Государство как заказчик услуг коммерческих ЦОДов
Приложение 1. Профили крупнейших коммерческих ЦОДов / Москва топ-10 / Санкт-Петербург топ-5 /Регионы топ-3	
Приложение 2. Международная и российская сертификация ЦОДов	
Приложение 3. Edge Computing: периферийные кЦОДы	
Приложение 4. Потребительские предпочтения на рынке кЦОДов	
Приложение 5. Экспортный потенциал российских дата-центров	

*В ходе работы над проектом возможны незначительные изменения структуры и объема отчета

Отчет дает углубленное представление о состоянии рынка коммерческих ЦОДов: от исторических показателей и наращиваемых и вводимых емкостей до анализа площадок по таким показателям, как возраст, число стоек, доходы, географическое расположение и региональные сегменты. iKS-Consulting представляет всю структуру игроков и рассматривает развитие рынка под влиянием различных факторов в целях реализации наиболее оптимального сценария его развития. Отчет дополнен информацией о региональном развитии рынка, основных трендах и перспективах развития.

Аналитическое исследование отечественного рынка услуг ЦОДов, ежегодно выполняемое специалистами iKS-Consulting, де-факто является одним из ключевых документов, которые помогают поставщикам услуг ЦОДов и их клиентам ориентироваться в текущей ситуации и оценивать перспективы развития своего бизнеса.

Более 15 лет iKS-Consulting находится в курсе всех событий, оказывающих влияние – как извне, так и изнутри – на спектр и качество услуг ЦОДов. Накопленная информация и экспертные наработки легли в основу авторской методики оценки социально-экономических показателей, на базе которой с достаточной высокой точностью строится прогноз на перспективу.

Параметры отчета

- Стоимость: 190 800 руб. (без НДС)
- Объем отчета: более 100 страниц
- Количество иллюстраций: более 50
- Дата выхода: сентябрь 2020

Подробная информация и заказ отчета

- АО «ИКС-холдинг»
- www.iKS-Consulting.ru
- E-mail: info@iks-consulting.ru
- Тел.: +7 (495) 150-64-24

IV ПРОФЕССИОНАЛЬНАЯ ПРЕМИЯ В ОБЛАСТИ ДАТА-ЦЕНТРОВ

RUSSIAN DATA CENTER AWARDS 2020

Торжественная церемония награждения состоится онлайн 10 декабря 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