ТЕМА НОМЕРА

АВАРИЙНОЕ ВОССТАНОВЛЕНИЕ И ОБЛАКА

ИнформКурьер-Связь
ИКС
издается с 1992 года

Константин Борман

Управляющий директор IXcellerate

IXcellerate

ЦОД - инвестиции в стабильность

Внутрирядные прецизионные кондиционеры InRow DX 300 мм второго поколения

- **Компактность и мощность;**
- **Высокая энергоэффективность;**
- **Адаптированность для использования на территории России.**

Решение предназначено для охлаждения коммутационных узлов, серверных помещений и ЦОДов.

Узнать подробнее об InRow DX 300 мм

www.apc.com

Life Is On

APC™ by Schneider Electric

Издается с мая 1992 г.

Издатель
ООО «ИКС-Медиа»

участник
АНО КС ЦОД

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

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

Главный редактор

А.Г. Барсков
a.barskov@iks-media.ru

РЕДАКЦИЯ
iks@iks-media.ru

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

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

Корректор
Е.А. Краснушкина

Дизайн и верстка
Е.В. Денисова

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

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

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

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

№3/2020 подписан в печать 31.08.20.
Тираж 8 000 экз. Свободная цена.
Формат 64x84/8

ISSN 0869-7973

12+

Время Tier IV?

В конце июля «Ростелеком – ЦОД» объявил о начале строительства в Москве ЦОДа Tier IV. Площадка вместит 2 тыс. стоек, причем первые 500 стойкомест введут в строй уже во второй половине 2021 г. Кроме того, по нашим данным, еще один игрок из топ-5 коммерческих ЦОДов реализует рядом с МКАД объект, который собирается сертифицировать по Tier IV.

Вообще говоря, ЦОДов, построенных и сертифицированных в соответствии с требованиями Tier IV, в мире немного – порядка 50. Причем существенная их часть – на Ближнем Востоке, где любят «золотые майбахи». Так, в Саудовской Аравии – шесть ЦОДов Tier IV, тогда как в США только четыре (два из них принадлежат одной компании – Switch). Но ЦОД Tier IV не только показатель «крутизны» его владельца. Более глубокий анализ показывает, что такие ЦОДы востребованы теми, кому нужна высокая надежность.

Дело в том, что Tier IV – это реальная отказоустойчивость. Собственно говоря, и в документах Uptime Institute этот уровень обозначен как Fault Tolerant. Ну а Tier III значит Concurrently Maintainable, т.е. это не гарантия отказоустойчивости, а возможность обслуживания без отключения полезной нагрузки.

Отказоустойчивость инфраструктуры ЦОДа Tier IV достигается за счет таких решений, как секционирование, непрерывное охлаждение и автоматизация. Поясню принцип секционирования. Например, если все ИБП (основные и резервные) находятся в одной комнате, то ее разрушение (скажем, затопление) означает остановку работы всего ЦОДа. В ЦОДе Tier IV ИБП надо разнести по разным комнатам так, чтобы авария в одной не отразилась на работе объекта. Для соответствия Tier IV подобный подход необходимо реализовать для всех систем, кабельных трасс, трубопроводов и т.д.

Серьезные аварии происходят не часто, поэтому показатели доступности у ЦОДов Tier III и Tier IV примерно равные. А поскольку Tier III и Tier IV обеспечивают одинаковые возможности обслуживания без прерывания предоставления сервисов, то становится понятно, почему подавляющее большинство ЦОДов – Tier III. Это просто «хороший мерседес».

Видимо, движение ведущих российских операторов ЦОДов в направлении Tier IV подкреплено запросами клиентов. ИТ-сервисы становятся настолько важными для компаний, что они готовы тратить дополнительные средства на услуги ЦОДов с гарантированной отказоустойчивостью. Ну а для оператора Tier IV – это еще и отличный способ выделиться на фоне конкурентов.

С пожеланием успеха проектам Tier IV в России,
Александр Барсков

ТЕМА НОМЕРА

Аварийное восстановление и облака

с. 34

с. 4

ЦОД как пятый элемент индустриальной недвижимости

с. 10

Т. Толмачева. Промышленный интернет в России-2020: на паузе

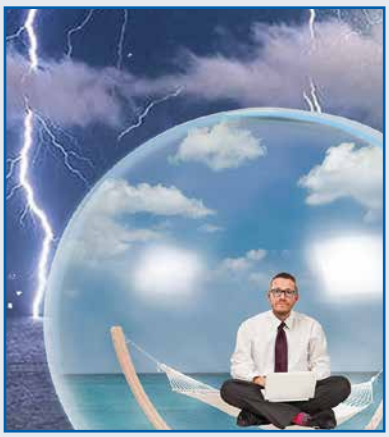
с. 55

Д. Оськин. IoT в зданиях: требуется единая сеть доступа

с. 74

Н. Носов. Рынок IaaS: время строить бренды

с. 88



М. Мустафаев. Как обеспечить безопасность бизнеса на «удаленке»

ЦОД как пятый элемент индустриальной недвижимости

Вода, электричество, газ, интернет и… ЦОД. Цифровая инфраструктура становится обязательным элементом современных предприятий. Яркий пример тому – цифровое оснащение комплекса Industrial City, открытого в начале июля губернатором Подмосковья Андреем Воробьевым в Подольске.

Одной из тенденций текущего этапа развития экономики является вывод производственных и логистических мощностей за пределы крупных городов. В московском регионе активно осваиваются привлекательные для индустриальной недвижимости территории вдоль основных вылетных магистралей и ЦКАДа, где строятся крупные производственно-складские комплексы. Один из них – Industrial City, расположенный на территории первого в России мультифункционального парка «Сынково».

Industrial City – это ИТ-заряженный промышленный коворкинг, где расположены 19 производственно-складских помещений с административно-бытовым корпусом, парковкой, охраной, инфраструктурой, благоустроенной территорией. Объем инвестиций в проект – 1 млрд руб.

«COVID отступает, на главные роли выходит экономика. Территория парка “Сынково” – 57 га, и она заполнена практически на 100%. Некоторые объекты еще сдаются, но на них уже есть покупатели или арендаторы, которые размещают компактные автоматизированные производства. В каждом цехе производится очень конкурентоспособная продукция, – заявил Андрей Воробьев. – Мы многое можем предложить инвесторам – землю бесплатно, компенсацию затрат на инфраструктуру. Есть комплекс льгот на имущество, налог на прибыль. Вода, электричество, газ – неотъемлемые части инфраструктуры. Здесь также есть сверхскоростной интернет, удобное хранение данных».

Действительно, наличие цифровой инфраструктуры – еще один важный тренд развития экономики. ИТ-системы становятся ключевыми, жизненно важными элементами для все большего числа предприятий, а для многих – основой производственных и бизнес-процессов. При этом все больше компаний отказываются от создания собственных ЦОДов, предпочитая размещать свои ИТ-системы в коммерческих дата-центрах.

Именно коммерческий ЦОД стал ключевым элементом инфраструктуры Industrial City в «Сынково». Его развернула компания 3data, известная своими ЦОДами «шаговой доступности» в Москве. Сейчас завершена первая фаза ЦОДа в «Сынково» (он получил наименование CA107), который реализован по модели франчайзинга и стал первым дата-центром 3data за пределами Москвы. Чтобы минимизировать риски, компания начала с небольшого ЦОДа, построенного на основе модульного решения, которое произведено питерской компанией GreenMDC.

Услуги ЦОДа оказались востребованы. Еще не все резиденты заехали в «Сынково», а ресурсы первой очереди ЦОДа (14 стоек) уже распроданы. Интерес к услугам проявили не только резиденты парка, но и компании и организации из близлежащих индустриальных зон. Сейчас 3data начинает второй этап реализации проекта, на котором будет построен классический дата-центр еще на 60 стоек – с проектной мощностью до 200 стоек. Тогда модульный ЦОД можно будет перевести в другое место, сохранив сделанные инвестиции.

«Площадка, расположенная на территории Подмосковья, не уступает по качеству московским дата-центрам и при этом обеспечивает близкое расположение вычислительной инфраструктуры для организаций, работающих в южных районах Московской области. По сути это сохранение основополагающего для нас принципа “шаговой доступности” ЦОДа»,– рассказывает Илья Хала, генеральный директор 3data.

Фото: Пресс-служба Губернатора и Правительства МО/К. Семенец

Производственно-логистический комплекс Industrial City

«Основные здания в Industrial City представляют собой ангары (для размещения производственного и складского оборудования), к которым пристроены офисные помещения, – продолжает он. – Специализированных помещений для ИТ-систем не предусмотрено. Поэтому наличие “под боком” профессионального ЦОДа – просто находка для резидентов. Тем более что их головные офисы часто находятся либо в Москве, либо вообще за границей. Высокооплачиваемые ИТ-специалисты из этих офисов могут дистанционно обслуживать системы, установленные в ЦОДе. Если смотреть из Москвы, то наш ЦОД отвечает модной концепции edge computing, а если из Подмосковья – то это ЦОД “шаговой доступности”».

Фото: Пресс-служба Губернатора и Правительства МО /К. Семенец

Андрей Воробьев (слева) и Илья Хала в ЦОДе CA107

Помимо собственно центров обработки и хранения данных ключевым элементом цифровой инфраструктуры являются надежные и высокопроизводительные каналы связи. С этим в Подмосковье не все было благополучно. «Стоит сделать шаг за МКАД, и качество инфраструктуры резко падает, – утверждает Виталий Езопов, генеральный директор оператора связи «Мастертел». – До недавнего времени обеспечить качественное подключение клиентов за МКАДом было сложно. Предоставляя услуги в Подмосковье, мы не могли гарантировать SLA. Ничего не оставалось, как самим совместно с партнерами заняться созданием собственной инфраструктуры связи, начиная со строительства кабельной канализации».

По данным, которые приводит В. Езопов, новой инфраструктурой охвачено уже порядка 40% всех основных объектов индустриальной недвижимости до ЦКАДа. По некоторым направлениям, например по Варшавскому шоссе, инфраструктура построена дальше «бетонки», на расстояние до 60 км от Москвы. При этом, как и в Москве, «Мастертел» подключает клиентов двумя оптическими линками, проложенными по разным маршрутам, что гарантирует отказоустойчивость и высокие показатели SLA. Стандартные кабели, используемые оператором, содержат 288 оптических волокон, что обеспечивает практически неограниченное масштабирование пропускной способности. На сегодня активно задействуются скорости вплоть до 100 Гбит/с.

По такой схеме подключен и ЦОД CA107. Помимо «Мастертела», якорного партнера 3data, на объект «зашли» и другие операторы. Как утверждают в 3data, ЦОД обеспечен оптическими соединениями со всеми основными бизнес-центрами и центрами обработки данных Москвы и Подмосковья, а также доступом к облачной инфраструктуре. Подобные ЦОДы становятся интересными операторам связи, поскольку могут служить эффективными точками подключений и коммутации, что чрезвычайно важно для развития цифровой инфраструктуры.

«Мы рассчитываем, что в наших ЦОДах в Подмосковье будут размещаться как крупные, в том числе сотовые, операторы, которые “идут в область”, так и региональные операторы, которым необходимы качественные аплинки в Москву», – полагает И. Хала.

Комментируя развитие ЦОДов 3data в Подмосковье, директор по развитию iKS-Consulting Дмитрий Горкавенко отмечает: «Такой подход для игрока рынка коммерческих ЦОДов оправдан, и это подтверждается нашими исследованиями. Сегодня ИКТ-инфраструктура крупного, в особенности промышленного, клиента чаще всего – в 65% случаев – гибридна. Обычно она включает основной/резервный корпоративный ЦОД (ЦОДы) – для старых и унаследованных ИТ-сервисов, корпоративных инфраструктурных сервисов и т.п., а также коммерческий ЦОД – для ИТ-сервисов, доступных из интернета (порталов самообслуживания), удаленных рабочих мест, новых ИТ-сервисов, телефонии, бэкапа, катастрофоустойчивости и т.п. Наличие географически разнесенных площадок особенно важно для производственных и торговых подразделений».

«3data хочет стать оператором “географически распределенной” площадки, увязывая региональные ЦОДы со своим облаком в единую инфраструктуру, оставляя заказчику только основной корпоративный ЦОД. С учетом плотной кооперации с «Мастертел» компания также закрывает вопрос связанности площадок. Получается инфраструктурный “бандл”, который очень интересен заказчикам», – добавляет эксперт iKS-Consulting.

По словам И. Халы, сегодня в Подмосковье в стадии проектирования и строительства на объектах индустриальной недвижимости находятся еще восемь ЦОДов 3data. Четыре их них планируется ввести в эксплуатацию уже в 2020 г. Эти восемь ЦОДов, которые территориально привязаны к основным вылетным магистралям, должны закрыть базовую потребность в узлах хранения и обработки данных. Всего же для Подмосковья, по оценкам Виталия Езопова, потребуется 20–25 таких дата-центров.

Александр Барсков

Время онлайн

CLOUD & DIGITAL TRANSFORMATION

ИТ-отрасль выдержала стресс-тест, устроенный пандемией. Цифровая трансформация помогла быстрому переходу на удаленную работу. Облачный рынок растет, опережая прогнозы, и значительно быстрее отрасли в целом.

Таков самый общий итог конференции Cloud & Digital Transformation 2020, организованной «ИКС-Медиа». Впервые самая популярная у специалистов облачного рынка страны конференция проходила в формате онлайн. Это положительно сказалось на числе участников – она привлекла около 600 делегатов со всей России.

Больше облаков

Переход на удаленную работу у компаний, которые уделяли внимание цифровой трансформации, в целом прошел гладко, без серьезных проблем. Огромную помощь в этом оказали облачные сервисы. Несмотря на негативное воздействие кризиса, облачный рынок продемонстрировал рост, причем значительно превышающий рост ИТ-отрасли в целом.

Так, по итогам первого квартала 2020 г. выручка облачного подразделения Amazon повысилась на 33%, Microsoft – 27%, Google Cloud – 50%. За второй квартал облачное подразделение IBM показало рост на 30%. «Мировые цифровые активы не просто переживают кризис, а делают это успешно. Это не отдельный хороший результат отдельной компании, а глобальный тренд», – подчеркнул руководитель направления по работе с корпоративными клиентами компании SberCloud Петр Предтеченский. Эксперт отметил увеличение запросов на облачные ресурсы SberCloud в категории «дайте прямо сейчас, цена второстепенна». Причем российский рынок стал больше интересоваться сложными сервисами PaaS, например, облачными инфраструктурными и платформенными сервисами для искусственного интеллекта, о которых рассказал руководитель департамента технологического консалтинга SberCloud Илья Сулейманов. На базе таких сервисов уже развернуты решения для борьбы с COVID-19.

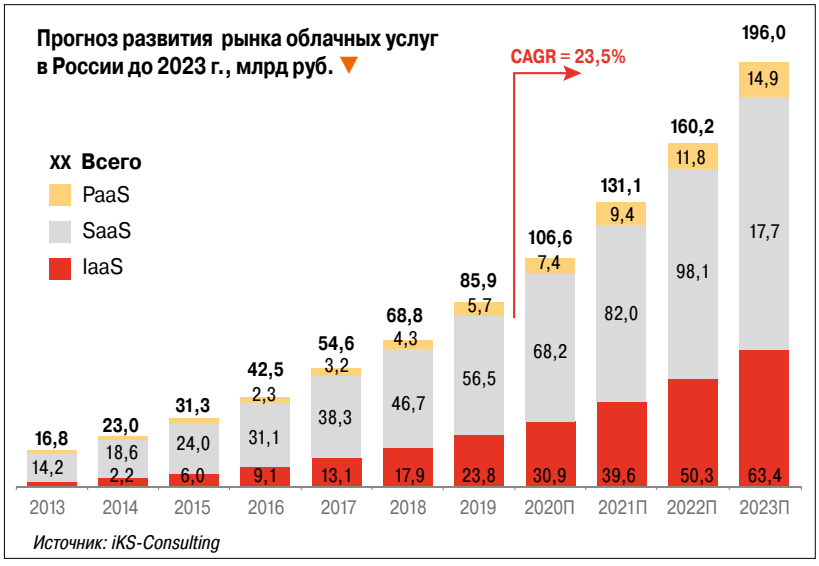
«С марта по апрель мы увидели стремление заказчиков срочно закрыть текущие потребности. Потом зафиксировали резкое, в два-три раза увеличение объемов нескольких серьезных контрактов в России, которые были заранее продлены. В разы вырос интерес к бэкапу Office 365», – сообщил региональный директор компании Veeam в России и СНГ Владимир Клявин.

Руководитель направления облачных продуктов компании «МегаФон» Алексей Извеков указал, что в условиях неопределенности компании замораживали запланированные стратегические мероприятия, имеющие отложенный экономический эффект. Но в целом повышенный спрос выживших компаний переломил негативные последствия, обусловленные ограничением ресурсов, которые выделялись на развитие, и сокращением числа клиентов из-за кризиса.

Значительно возрос спрос на клиентские устройства. Резко увеличили закупки «тяжелого» серверного оборудования гиперскейлеры. «Мы увидели существенный рост продаж “тяжелых” процессоров типа Intel Xeon Gold – заказчики решили консолидировать мощности в датацентрах, ориентированных на онлайн-общение. Что касается России, план продаж на первую половину 2020 г. значительно перевыполнен», – пояснил менеджер по развитию бизнеса компании Intel Василий Лизунов.

Облачное завтра

По данным совместного опроса iKS-Consulting и Intel, 61% российских компаний считают влияние эпидемии COVID-19 на ИТ-процессы предприятий существенным, 93% занялись организацией удаленных рабочих мест, закупкой дополнительного оборудования и ПО, 82% полагают, что удаленная работа частично сохранится и после окончания пандемии, и более половины рассматривают



Источник: iKS-Consulting

переход в облака в качестве наиболее актуального технологического направления развития компаний (подробнее см. с.79).

Помимо пандемии на рост российского облачного рынка оказывают влияние процессы цифровой трансформации общества и бизнеса, национальный проект «Цифровая экономика». Эксперты iKS-Consulting прогнозируют, что отечественный рынок облачных услуг к 2023 г. вырастет в 2,3 раза до 196 млрд руб. Он будет увеличиваться не менее чем на 23% ежегодно, при этом ожидается, что отдельные сегменты будут прирастать на 30–31% в год.

Как отметил директор по развитию бизнеса iKS-Consulting Дмитрий Горкавенко, на пути цифровой трансформации экономики в России есть ряд препятствий: нехватка квалифицированных кадров, недостаток финансовых ресурсов и отсутствие единого понимания самого процесса цифровой трансформации. Тем не менее отечественный рынок облачных услуг переходит к этапу зрелости, с задержкой на два-три года повторяя изменения в структуре, происходящие в мире. Россия становится экспортером облачных услуг – доля зарубежных клиентов в выручке российских облачных провайдеров в 2019 г. составляла 4,1% в секторе IaaS, 6,7% в секторе SaaS и продолжала расти.

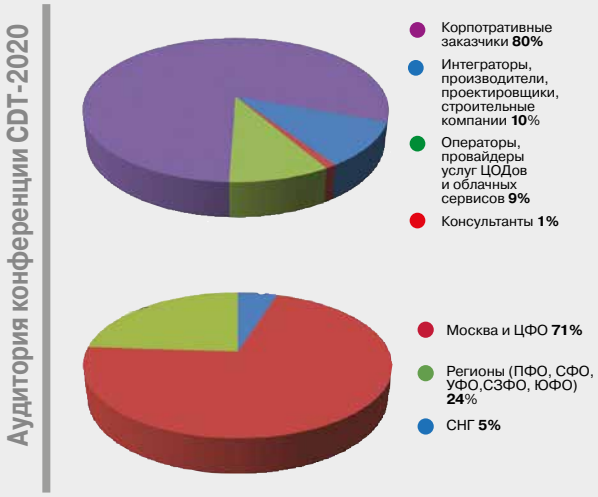
Дорога в регионы

Одной из ключевых тенденций 2021 г. станет релокация облачных ресурсов крупнейших операторов в регионы и одновременно рост в регионах спроса на облачные услуги. Свое решение для распределенных облачных вычислений, которое предполагает их выполнение с помощью территориально распределенных вычислительных ресурсов, находящихся в «шаговой доступности» от потребителей, предлагает компания CDNVideo. Ее ноу-хау – балансировщик нагрузки, минимизирующий задержки за счет оптимального выбора узла распределенной облачной платформы. Первыми коммерческими клиентами услуг распределенных вычислений в регионах могут стать набирающие популярность сервисы облачного гейминга.

Повысить надежность и производительность работы региональных пользователей с зарубежными облаками гиперскейлеров помогут сервисы Linxdatacenter на базе платформы Equinix Cloud Exchange. Клиент получает выделенный канал с гарантированной скоростью и качественными характеристиками.

Cloud & Digital Transformation расширяет аудиторию

Спикеры собрались в студии в Москве, а делегаты слушали онлайн-трансляцию через интернет и задавали вопросы в чате. Такая схема при соблюдении всех противоэпидемических норм позволила, с одной стороны, обеспечить свойственную офлайновым мероприятиям профессиональную атмосферу, столь важную для спикеров, а с другой – поучаствовать в онлайне максимально большому числу делегатов, в том числе находящихся далеко от Москвы. 80% делегатов представляли корпоративных заказчиков, причем почти четверть участников оказалась из российских регионов, около 5% – из стран СНГ.



Экзамен сдан

Пандемия стала сильнейшим испытанием для ИТ-отрасли страны. «Наберусь смелости сказать за весь ИТ-рынок России – стресс-тест дал положительный результат, практически все оказались к нему готовы», – заявил директор по информационным технологиям компании «Кораблик» Артем Елизаров. Бизнес активно стал взаимодействовать с партнерами и клиентами через интернет. Как отметил системный инженер Western Digital Григорий Никонов, практически ниоткуда выросла новая вертикаль – телемедицина.

После ослабления ограничительных мер люди снова начали ходить в магазины, но по-прежнему многие покупки осуществляются в сети. Некоторые бенефициары, например телевидение, после роста в апреле на 70% (по данным трафика клиентов CDNVideo) в июне вернулись к февральским показателям. Но в целом рост сохранился. Интернет-кинотеатры показали в июне прирост относительно февраля на 30% (в апреле – 40%), электронная коммерция – на 52% (в апреле – 80%), дополнительное образование – 115% (139%), СМИ – 15% (131%), развлекательные ресурсы – 14,7% (22%). Пандемия подхлестнула процессы цифровой трансформации, после нее мир уже не станет прежним. Наступает время онлайн.

Николай Носов

НОВОСТИ АНО КС ЦОД

ИЮНЬ 2020.

Новый участник АНО КС ЦОД

В число участников АНО КС ЦОД вошла компания CDNVideo — ведущая сеть CDN в РФ. Узлы сети установлены в 20 городах России, а также на Украине, в Белоруссии, Казахстане, Узбекистане, Молдавии, Азербайджане, Германии, Нидерландах, США и Сингапуре. Кроме того, CDNVideo оказывает услуги георасределенного облака и занимается созданием частных облаков под ключ.

ИЮЛЬ 2020.

АНО КС ЦОД приняла участие в заседании Комитета РСПП по цифровой экономике

Онлайн-заседание прошло с участием Комиссии РСПП по связи и информационно-коммуникационным технологиям, Комиссии РСПП по электроэнергетике, Министерства цифрового развития, связи и массовых коммуникаций РФ, Министерства энергетики РФ, Министерства экономического развития РФ и Центра компетенций по направлению «Информационная инфраструктура» программы «Цифровая экономика РФ». С основным докладом «О мерах совершенствования механизмов электроснабжения ЦОДов» выступил генеральный директор АНО КС ЦОД Дмитрий Бедердинов.

Он подчеркнул, что сегодня практически отсутствует возможность для оптимизации тарифов ЦОДов и это «не позволяет сделать качественный скачок в развитии индустрии».

НОВОСТИ ОТРАСЛИ

Мобильные ЦОДы – в Индию, гиперЦОД – в Москву

«Росатом» ведет переговоры о поставках мобильных дата-центров в Индию. Хотя компания занялась контейнерными и мобильными ЦОДами, она не собирается сворачивать проекты строительства опорных ЦОДов при атомных станциях (первым таким объектом стал дата-центр, построенный вблизи Калининской АЭС в Тверской области в 2018 г.). В мае «Росатом» объявил о подписании соглашения с ФСК ЕЭС о создании гиперЦОДа (ориентировочно на 2 тыс. стоек) в Москве.

Новый руководитель IXcellerate в России

В середине мая IXcellerate, занимающая второе место в составляемом iKS-Consulting рейтинге коммерческих ЦОДов России, объявила о назначении Константина Бормана на должность управляющего директора. Его профессиональный опыт превышает 25 лет, причем последние 15 лет он занимал руководящие позиции в крупнейших коммерческих дата-центрах Европы и Азии, среди которых такие известные международные компании, как Interxion, Virtus и Chayora.

Амбициозные цодостроительные планы Украины

Украинское Министерство энергетики и защиты окружающей среды рассматривает возможность создания ЦОДов рядом с АЭС. Пилотный проект присоединения потребителей ЦОДа мощностью до 1 ГВт к электрическим сетям с выделением первой очереди 30 МВт разработан в Энергодаре, городе – спутнике Запорожской АЭС. Также НАЭК «Энергоатом» помимо проекта с Запорожской АЭС рассматривает возможность строительства вблизи Ривненской атомной станции ЦОДа мощностью до 50 МВт с дальнейшим ее наращиванием свыше 200 МВт.

«Ростелеком» строит региональный ЦОД в Южно-Сахалинске

ЦОД поможет обеспечить вычислительными ресурсами и системами хранения данных государственный сегмент и представителей бизнеса Сахалинской области. Ввод в эксплуатацию планируется осенью 2020 г. На начальном этапе мощность ЦОДа составит 1,5 МВт, емкость машинных залов – 25 стойко-мест.

Свет для ЦОДов

Минкомсвязь России подготовила проект постановления правительства, которое позволит предоставить операторам ЦОДов льготный доступ на рынок электрической энергии и мощности с 1 января 2021 г. В проекте предлагается для этих организаций установить минимальную сбытовую надбавку, покрывающую подтвержденные расходы генерирующей и транспортирующей стороны. Кроме того, объекты сетей связи (в том числе дата-центры), если их суммарная присоединенная мощность равна или превышает 670 кВт, смогут получить статус субъекта оптового рынка.

«Газпром нефть» формирует собственный ИТ-кластер

В состав кластера войдут три технопарка в Санкт-Петербурге, Омске и Ноябрьске, четыре центра обработки данных и около 20 технологических представительств в более чем 30 регионах страны. В целом в ИТ-кластере будут заняты почти 6 тыс. специалистов.

Фото: «Газпром нефть»

Технопарк промышленной автоматизации «Газпром нефти» в Омске

Планы развития GreenBush DC

Резидент ОЭЗ «Технополис «Москва» компания «ГДЦ Энерджи Групп» до 2023 г. направит около 2,8 млрд руб. на развитие коммерческого ЦОДа GreenBush DC. Сейчас в машинных залах центра на площадке «Алабушево» общей площадью 2 га размещаются 660 стоек обработки информации с максимальной нагрузкой на одну стойку до 20 кВт. К концу 2023 г. компания планирует запустить в эксплуатацию 2280 стоек.

Фото: GreenBush DC

ЦОДу Tier IV в России быть!

«Ростелеком – ЦОД» приступил к строительству дата-центра в Москве с максимальным уровнем надежности (Tier IV). Новый дата-центр появится на юго-востоке Москвы. При общей площади 10 150 кв. м он вместит 2 тыс. стоек мощностью 5 кВт каждая. Общая мощность дата-центра составит 17 МВт. Дата-центр будет вводиться в эксплуатацию поэтапно: первые 500 стойко-мест запустят во второй половине 2021 г. Выход на полную мощность намечен на середину 2022 г.

КОЛОНКА ЭКСПЕРТА

КОНСТАНТИН БОРМАН,
управляющий директор в России, IXcellerate

ЦОД – ЭТО ВСЕГДА БОЛЬШИЕ ИНВЕСТИЦИИ

Как получить финансирование на строительство и расширение ЦОДов? Какие инвестиции наиболее привлекательны? На что уходят деньги?

Строительство и расширение дата-центров – это капиталоемкие проекты, которые требуют больших инвестиций. Согласно данным Gartner, в прошлом году на инфраструктуру дата-центров в мире было потрачено $205 млрд. Российский рынок развивается намного быстрее мирового: по оценке iKS-Consulting, он растет на 30% в год, выручка российских провайдеров услуг ЦОДов в 2018 г. составила 28,5 млрд руб. ($458 млн).

Если бизнес новый и строительство планируется с нуля, у компании нет клиентов и уже действующего ЦОДа, то единственный способ привлечения денег – это прямые инвестиции (private equity). Со временем, когда бизнес приобретет определенный размах, возможна смешанная модель финансирования с привлечением кредитов (debt financing), которые компания может использовать для пополнения оборотного капитала или для будущих капиталовложений в развитие инфраструктуры.

Возможности финансирования и стоимость денег сильно различаются от региона к региону, например, между Россией и Европой разница колоссальная. На развитых финансовых рынках с устоявшимся бизнесом дата-центров можно получать кредиты под развитие бизнеса на достаточно гибких условиях. После достижения определенного уровня доходов и EBITDA (полученная прибыль до вычета процентов, налога на прибыль и амортизации активов) объем займа может рассчитываться исходя из величины EBITDA, умноженной на определенный коэффициент (мультипликатор), который может варьироваться от 3,5 до 4,5.

В России в большинстве случаев применяется другая схема финансирования кредитов. Получение займов идет через банки, которые почти всегда требуют залога, чаще всего в виде недвижимости и акций компании. Причем в зависимости от банка размер залога (обременения) может во много раз, даже десятикратно, превышать объем займа. Банки требуют таких гарантий, чтобы обезопасить себя от неплатежей и банкротств. Вероятно, практика кредитования в России и возможности более гибкого финансирования перспективных отраслей, какой является индустрия ЦОДов, – это один из тех вопросов, который необходимо адресовать правительству при обсуждении мер поддержки развития экономики, чтобы способствовать изменению законодательства и появлению более гибких моделей финансирования по аналогии с европейскими. Это в значительной степени ускорило бы развитие и потенциально снизило стоимость капитала, особенно для среднего бизнеса и стартапов, – не только компаний, которые занимаются инфраструктурным бизнесом, но и, например, разработчиков ПО. В настоящий момент из-за определенных льгот (в частности, НДС), под которые подпадают зарубежные программные продукты, отечественные разработчики не всегда могут успешно конкурировать с ними.

По законам рыночной экономики операторы ЦОДов должны концентрироваться на развитии бизнеса и генерации выручки. Оптимальным вариантом для многих является привлечение инвестиций под гарантии будущих доходов и подписанные контракты с клиентами. Сегодня существует явный разрыв между спросом на рынке капитала и предложением банков, которые в связи с обязательством внести залог навязывают заемщикам кабальные условия с ограниченными перспективами дальнейшего наращивания объемов финансирования.

В Европе, если у заемщика, оператора ЦОДа, уже есть клиенты, инвестиции обычно можно получить в комбинации: 40% – по модели private equity и 60% – debt financing. Как правило, кредиты берутся на срок от трех до пяти лет, иногда на более длительный срок, что позволяет развивать бизнес и получать дополнительное финансирование по мере его роста. Также стоимость капитала сильно различается в разных регионах. В России доступные на рынке капитала ставки финансирования для среднего бизнеса составляют 8–10% годовых, а для мезонин-финансирования ставка может возрасти до 20% и более. Для сравнения: в Европе ставки финансирования могут быть в два-три раза ниже.

Так как строительство ЦОДов требует больших капитальных вложений, операторы должны тщательно планировать возведение новых объектов для оптимизации инвестиций и снижения рисков. Львиная доля затрат – до 90% – приходится на инфраструктуру ЦОДов, включая энергообеспечение, закупку и установку инженерного оборудования. Остальные средства идут на аренду или покупку земли, а также покупку или строительство здания.

Если оператор собирается эксплуатировать ЦОД по модели retail colocation (сдача в аренду от одной стойки), то маржинальность такого бизнеса выше и можно ожидать, что внутренняя норма рентабельности составит 20–25%. Если планируется масштабное строительство под конкретного клиента (от 2 МВт и более на одного заказчика), то объемы бизнеса могут быть выше, но это будет оптовый проект с эффектом масштаба, снижающим прибыль.

Промышленный интернет в России-2020: на паузе

Татьяна Толмачева,
партнер, iKS-Consulting

Рынок IIoT в России продолжает оставаться рынком «пионеров» и инноваторов. Недостаточная зрелость технологий сдерживает его рост, а спад промышленного производства, обусловленный пандемией и экономическим кризисом, повлечет за собой его сокращение.

Рынок промышленного интернета вещей неоднороден, как неоднороден и сам сектор промышленного производства. Каждая подотрасль использует свой набор технологических решений на базе IoT, поэтому рынок IIoT целесообразно рассматривать в разрезе основных секторов промышленности.

Едем тише…

Важно отметить, что развитие рынка промышленного интернета вещей зависит от динамики самого сектора промышленного производства, поскольку затраты на внедрение новых цифровых технологий закладываются, как правило, в бюджет ИТ-развития. А когда выручка предприятия стагнирует или падает, бизнес очень сдержанно подходит к инвестициям в новые проекты, и не важно, к какой сфере они относятся.

По данным Росстата, в 2019 и 2020 гг. рост промышленного производства в России в целом и по отдельным секторам замедлился: в 2019 г. производство увеличилось лишь на 2,4% против 2,9% в 2018 г., а в мае 2020 г. – сократилось на 9,6% по сравнению с маем 2019-го. Самые высокие темпы падения продемонстрировал сырьевой сектор.

Вследствие снижения объема промышленного производства уменьшаются и ИКТ-затраты. Средства в такой ситуации выделяются в основном на поддержку и эксплуатацию существующих ИКТ-систем, а не на внедрение новых. Например, в 2018 г. затраты на оплату услуг сторонних организаций и специалистов, связанных с ИКТ (кроме услуг связи и обучения), в промышленном производстве сократились почти на 30% относительно 2017 г. (данные Росстата).

Status quo

Технологии автоматизации уже давно активно используются в промышленности для выполнения ключевых производственных функций, в том числе технического обслуживания и снабжения комплектующими, управления персоналом, охраны труда, управления транспортными производственными средствами. Наиболее высок уровень автоматизации в добывающей промышленности, отдельных секторах обрабатывающей промышленности, в промышленной энергетике (рис. 1). Эти отрасли имеют крупнейшие среди всех отраслей промышленности ИКТ-бюджеты (рис. 2).

Предприятия этих отраслей уже давно используют информационные системы автоматизации производства типа MES, АСУ

Рынок IIoT – это рынок ИКТ-решений для цифровизации деятельности промышленного предприятия с использованием управляемого через интернет оборудования, сенсоров, датчиков, других средств производства, а также инструментов интеграции этих элементов между собой.

Источник: Росстат, 2018 г.

▲ **Рис. 1. Уровень автоматизации предприятий отраслей промышленного производства в разрезе бизнес-функций**

Источник: Росстат, 2018 г.

▲ Рис. 2. Крупнейшие отрасли промышленности РФ по объему ИКТ-затрат, млрд руб.

ТП, ERP, CSM и пр. Это востребовано бизнесом, поскольку позволяет заметно снижать производственные затраты. Не случайно основная масса проектов IIoT, которые были осуществлены в 2018–2019 гг. (рис. 3), относилась к секторам промышленного производства, упомянутым на рис. 2.

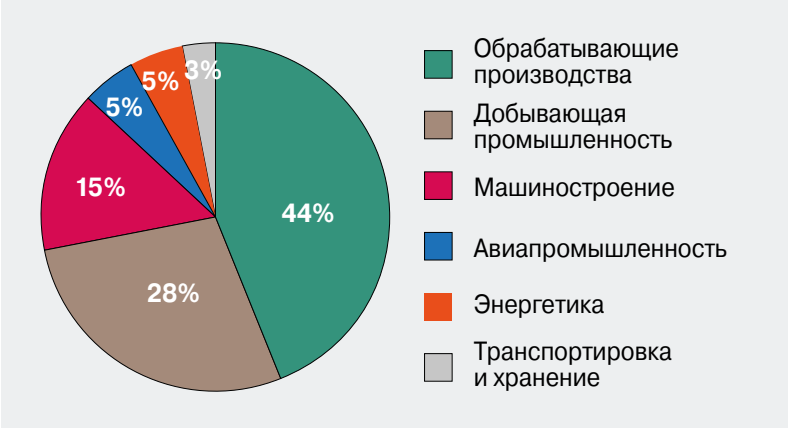
В число компаний, реализовавших в 2019 г. те или иные IIoT-проекты, входят «ЕВРАЗ Качканарский ГОК», «Лукойл-НК», разрез «Нерюнгринский», угледобывающая компания «Ресурс», а также «Роснефть», «Русский уголь», «СУЭК-Хакасия», «УК «Татбурнефть», ХК «Якутуголь». «Роснефть» в соответствии со своей стратегией цифровизации выполняет целый ряд программ: «Цифровое месторождение», «Цифровой завод», «Цифровая АЗС» и «Цифровая цепочка поставок». «Газпром нефть» разработала дорожную карту внедрения в компании технологий дополненной и виртуальной реальности (AR/VR). СУЭК охватила цифровыми технологиями все ключевые направления функционирования компании – интеграцию систем разведки, 3D-моделирование, диспетчеризацию всего горнодобывающего процесса и логистического цикла.

Среди машиностроительных компаний, вовлеченных в IIoT-проекты, можно назвать НПП «Грань», «ОДК-Авиадвигатель» и «ПКО Теплообменник». Можно также отметить стратегическое соглашение в сфере цифровых технологий для тяжелого машиностроения между ГК «Цифра» и УК «УЗТМ-КАРТЭКС», осуществляющей стратегическое управление производственными активами Газпромбанка. На площадках «ИЗ-КАРТЭКС им. П.Г. Коробкова», «ОМЗ – Литейное производство» и Уралмашзавода будет внедряться система мониторинга станков «Диспетчер», разработанная «Цифрой». Рассматривается возможность реализации совместных проектов в области искусственного интеллекта.

Отдельные промышленные предприятия сегодня переходят к следующему этапу автоматизации – к созданию сквозного информационного пространства, полной цифровизации ключевых производственных процессов добычи, транспортировки и переработки полезных ископаемых с использованием более сложных «умных» технологий (ИИ и машинного обучения, AR/VR, высокопроизводительных вычислений и пр.) на уже автоматизированных участках бизнес-процессов. Все эти новые технологии требуют сбора и обработки данных с промышленного оборудования. Правда, столь глубокую цифровизацию могут себе позволить только крупные компании, уже обеспечившие достаточно высокий уровень автоматизации большинства своих бизнес-процессов.

Удел пионеров

Большой разрыв в уровне проникновения IoT-технологий наблюдается как между подотраслями промышленности, так и между компаниями внутри одной отрасли.



◀ Рис. 3. Отраслевая структура реализованных в РФ в 2019 г. проектов IIoT (по числу проектов)

Источник: iKS-Consulting

По оценкам iKS-Consulting, объем рынка промышленного интернета вещей в 2019 г. увеличился на 4% до 7,92 млрд руб.* (рис. 4) при росте объема промышленного производства на 3%. Массового внедрения коммерческих проектов IIoT в 2019 г. не наблюдалось.

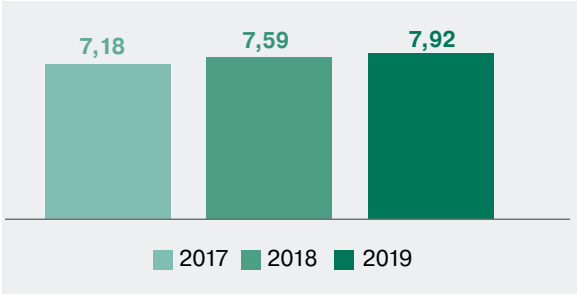
Ожидается, что драйвером внедрения цифровых технологий в промышленности в 2020–2024 гг. станут государственные инициативы по цифровизации промышленности и развитию сквозных цифровых технологий (СЦТ).

Осенью 2019 г. в конкурсном отборе Минпромторга на право получения из федерального бюджета субсидий с целью возмещения части затрат на разработку цифровых платформ на базе СЦТ было выбрано почти 90 компаний. Общий объем финансирования в 2019 г. был определен дорожной картой развития «сквозной» цифровой технологии «Новые производственные технологии» на уровне 2 млрд руб. Правда, по состоянию на май 2020 г. отобранные предприятия получили подтверждение финансирования своих проектов, но не само финансирование.

Другой драйвер роста – деятельность отдельных компаний (разработчиков IIoT-решений, интеграторов, операторов связи), которые избрали IIoT в качестве одного из стратегических направлений своего бизнеса. Таких компаний пока немного, например, ГК «Цифра», «Ростелеком», Mail.ru со своей платформой промышленного интернета вещей, системные интеграторы, имеющие выделенное направление промышленности.

Технологические вендоры (зрелые и стартапы) выводят и тестируют новые решения IoT на базе искусственного интеллекта, AR/VR, высокопроизводительных вычислений. Большая часть таких проектов находится на этапе пилотов. Например, «Сибур Холдинг» тестирует платформу для взаимодействия подразделений технического обслуживания и удаленных экспертов с применением дополненной реальности, а «Славнефть-Мегионнефтегаз» – с платформой «ИКСАР» (XR) для контроля за состоянием оборудования. Однако компания «Северсталь», запустив прототип интерактивного помощника для обслуживания оборудования, позднее прекратила его использование. Это свидетельствует о незрелости, а стало быть, ненадежности новых решений на базе «умных» технологий, что, очевидно, неприемлемо для сложных производственных процессов.

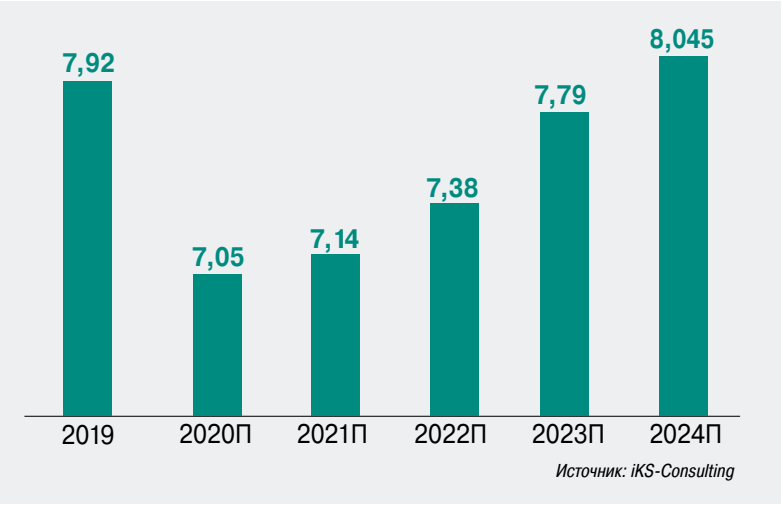
Таким образом, рынок IIoT растет, но очень медленно. Надежды на ускорение роста связывались с улучшением экономической ситуации**, но спад в экономике, который не может быть компенсирован государственными программами развития цифровых технологий, напротив, является тормозом.



◀ Рис. 4.
Объем рынка IIoT в РФ, млрд руб.
Источник: iKS-Consulting

* В статье Т. Толмачевой и Е. Ершовой «IIoT в России: от эволюции к революции» («ИКС» № 1'2019, с. 19) из-за различия в методиках оценки рынка цифры отличаются от приведенных. Оценка объема рынка, использованная в данной статье, определяется объемом потребительского спроса или, другими словами, объемом затрат предприятий всех подотраслей промышленности на внедрение решений IIoT. До 2018 г. объем рынка IIoT оценивался как суммарная выручка поставщиков решений от реализации проектов в сфере IIoT на предприятиях добывающей и обрабатывающей промышленности.

** Толмачева Т. ProIoT: «как много в этом звуке...». «ИКС» № 3'2018, с. 18.



▲ Рис. 5. Прогноз развития рынка IIoT в России, млрд руб.

Перспективы-2024

iKS-Consulting прогнозирует, что в 2020 г. рынок промышленного интернета вещей сократится почти на 11% до уровня 2017 г. и восстановится не ранее 2024 г. (рис. 5).

Основная причина – ожидаемое сокращение промышленного производства, обусловленное пандемией и экономическим кризисом. Минэкономразвития РФ прогнозирует падение промышленного производства в России по итогам 2020 г. на уровне 5,4%, а затем, в 2021–2023 гг., ежегодный рост на 3,3–3,4%. В 2020 г. вследствие неблагоприятных политических и экономических факторов, а также потепления климата, из-за которого снижается потребление углеводородов, сильнее всего сократится нефтегазовый сектор.

По оценке iKS-Consulting, ИКТ-бюджеты, направляемые на автоматизацию и цифровизацию производства, уменьшатся в 2020 г. почти на 5%. В такой ситуации промышленное производство могут поддержать федеральные расходы на нацпроекты, а значит, меры государственной финансовой поддержки для разработчиков сквозных цифровых технологий и промышленных предприятий, которые их внедряют, приобретут еще бóльшее значение. В июне 2020 г. президент дал поручение правительству РФ обеспечить необходимое финансирование федерального проекта «Искусственный интеллект», в том числе из средств федерального бюджета, предусмотренных на реализацию национальной программы «Цифровая экономика РФ».

Помимо государственных программ есть программы для высокотехнологичных стартапов, разрабатывающих решения на базе СЦТ в промышленности с участием бизнеса, например:

- программа поддержки «Промтех», организованная фондом «Сколково» и Инновационным центром «Ай-Теко». Среди направлений отбора – технологии удаленного управления предприятием, включая MES-системы, цифровые двойники, AR/VR;
- корпоративный акселератор проектов в сфере металлургии Severstal SteelTech Accelerator;
- «Цифровая лаборатория Норникеля».

Развитие промышленного интернета в России связывают с развитием сетей 5G, благодаря которым, как ожидается, повысится эффективность облачных хранилищ и вычислений по требованию, расширятся возможности использования искусственного интеллекта в интересах различных отраслей промышленности. Таким образом, драйвером роста и важной технологической основой для дальнейшего развития IIoT в России станут 5G, технологии ИИ и облачные вычисления.

Можно рассчитывать, что число проектов в промышленности, опирающихся на технологии машинного обучения и искусственного интеллекта, будет увеличиваться. Пока подобные проекты немногочисленны. Серьезный сдерживающий фактор, как и в случае IIoT-проектов, – незрелость технологий. Цена ошибки на производстве при внедрении «сырой» технологии намного выше, чем, скажем, в финансах или ритейле. Да и стоимость владения такой технологией на данном этапе достаточно высока.

Тем не менее в 2020–2022 г. будут активно развиваться технологические тенденции, наметившиеся в 2019 г.:

- переход от узких отраслевых решений к индустриальной цифровой платформе. Платформы дают больше возможностей, чем просто подключенные к интернету вещей устройства;
- рост интереса к технологиям робототехники и роботизированному безлюдному производству, безлюдной добыче, роботизированной транспортировке;
- распространение дистанционных систем управления персоналом, организация дистанционного обслуживания.

Росту популярности этих направлений будут также способствовать тенденции, которые проявились в период эпидемии коронавируса и введенных из-за нее ограничительных мер.

Таким образом, события 2020 г. окажут на рынок IIoT не только негативное влияние: они подтолкнут к автоматизации бизнес-процессов, обеспечивающей устойчивость производства и позволяющей высвобождать из этих процессов людей. Все бизнес-процессы будут анализироваться на предмет того, можно ли в них заменить человека «цифровым» работником или же его участие неизбежно. Параллельно автоматизация производственных процессов позволит решить проблему промышленной безопасности персонала. ИКС

ЖКХ как арена внедрения интернета вещей

Рынок «умного» ЖКХ в России находится на начальной стадии развития, на стадии пилотных проектов, формирования экосистемы игроков, принятия нормативной правовой базы. Однако удар по экономике, нанесенный пандемией коронавируса, замедлит рост рынка.

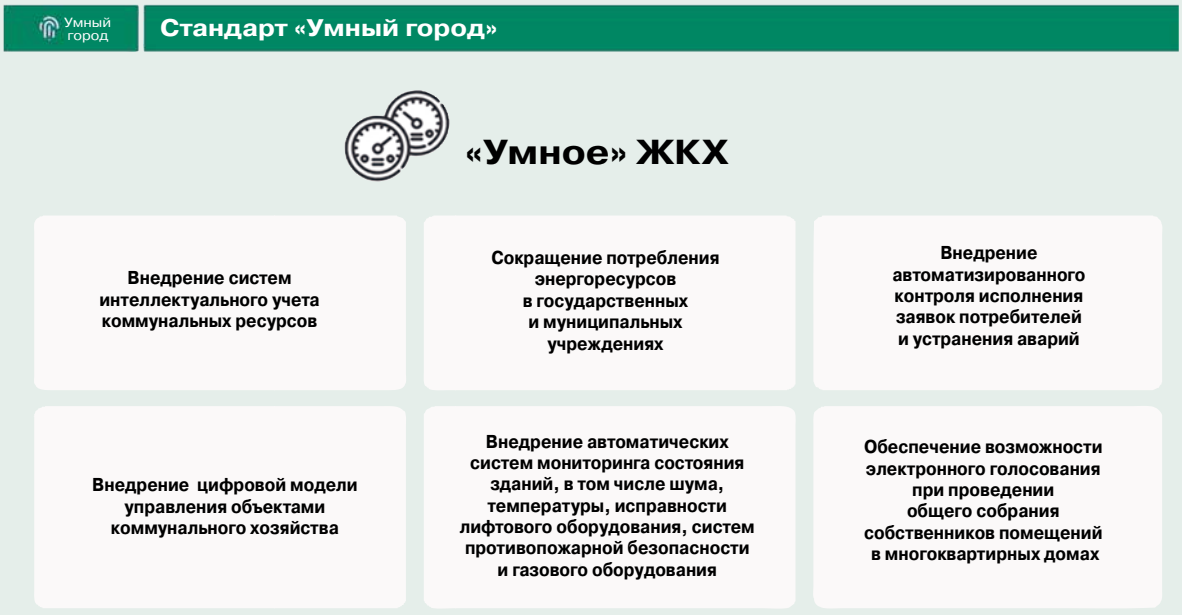
Николай Носов

«Умное» ЖКХ

Жилищно-коммунальное хозяйство – перспективная область внедрения решений интернета вещей. В новых технологиях заинтересованы все стороны. Жильцам не надо будет помнить о дате отправки показаний счетчиков и снимать показания с зачастую неудобно расположенных приборов, коммунальные службы смогут оперативно получать информацию о потребленных ресурсах. А ЖКХ – это не только снабжение электроэнергией, газом, теплом и водой, работа канализации. Это и вывоз и утилизация мусора, лифтовое хозяйство, уборка мест общего пользования, дорог и придомовых территорий, содержание зданий и вызвавший так много дискуссий в обществе капитальный ремонт. И всюду есть место для автоматического сбора информации о работоспособности и состоянии систем и последующей ее аналитической обработки – всего того, чем так привлекателен интернет вещей.

За рубежом рынок интернета вещей для ЖКХ активно развивается. Например, компании Eddy Home и Semtech предложили счетчики для домов и квартир, которые онлайн собирают и обрабатывают данные о потреблении воды. Владельцы жилых помещений через мобильное приложение своевременно оповещаются о протечках, резком перепаде температуры и влажности. В августе 2018 г. провайдер Vodafone Germany и немецкая Thyssenkrupp оборудовали более миллиона лифтов по всему миру SIM-картами для прогностического обслуживания и сокращения времени простоя.

Пользуются популярностью системы энергосбережения. Согласно прогнозам Frost & Sullivan, в Евросоюзе объем рынка управления спросом на электроэнергию благодаря развитию IoT и других новых технологий вырастет к 2025 г. до $3,5 млрд.



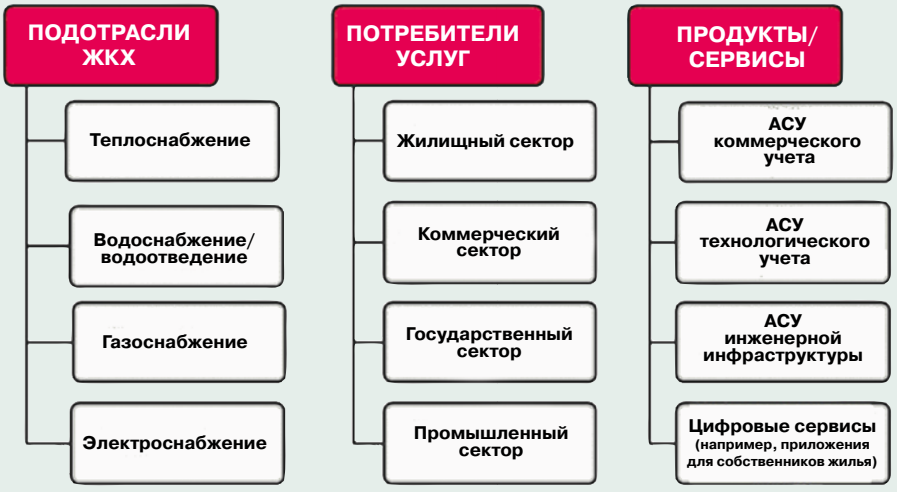
◀ **Рис. 1. «Умное» ЖКХ в рамках стандарта «Умный город»**

Источник: Минстрой России

1. Наличие системы интеллектуального учета
2. Доля МКД, оснащенных АСУ учета потребления ресурсов
3. Наличие систем мониторинга состояния зданий
4. Доля МКД, оснащенных системами мониторинга состояния зданий
5. Использование электронного голосования при проведении общих собраний

▲ Рис. 2. Индикаторы «умного» ЖКХ

Источник: Минстрой России



▲ Рис. 3. Группы игроков рынка «умного» ЖКХ

Источник: iKS-Consulting

Границы рынка

В принятом в начале 2019 г. Министерством строительства и жилищно-коммунального хозяйства РФ ведомственном стандарте «Умный город» есть отдельное направление – «умное» ЖКХ, определившее границы нового рынка. Маркетинговый термин «умное» ЖКХ получил «законодательное» закрепление через набор технологических решений для внедрения интеллектуальных систем управления инфраструктурой, жилфондом и социальными объектами, направленных на повышение эффективности энергетической и коммунальной инфраструктуры, снижение издержек ресурсоснабжающих организаций.

Для «поумнения» ЖКХ предлагается внедрить системы интеллектуального учета ресурсов, автоматизированного дистанционного управления, интеллектуального управления инфраструктурой, платформы электронного голосования собственников многоквартирных домов (МКД), оцифровку объектов инфраструктуры, планирование инвестиционных и производственных программ с применением интеллектуальных систем прогнозирования аварий (рис. 1).

Методика расчета «IQ» городов, утвержденная приказом Минстроя России, закрепила пять индикаторов, которые определяют уровень «ума» ЖКХ (рис. 2).

Партнер iKS-Consulting Татьяна Толмачева выделяет три группы игроков нового рынка: подотрасли ЖКХ (теплоснабжение, водоснабжение и отведение, газоснабжение), потребители услуг (жилищный и коммерческий сектор, государство и промышленность) и разработчики продуктов и сервисов – автоматизированных систем инженерной инфраструктуры, коммерческого и технологического учета, различных цифровых сервисов (рис. 3).

Показатели рынка

Состояние рынка цифрового ЖКХ в жилом секторе оценивается через показатель проникновения цифровых приборов учета потребления коммунальных ресурсов. В ГИС ЖКХ зарегистрировано 1,4 млн МКД, 18,9 млн жилых домов, 618 тыс. управляющих компаний и 51 тыс. товариществ собственников жилья. Это целевая аудитория, для которой разрабатываются цифровые решения и продукты.

Общий уровень оснащенности приборами учета в России пока низок. Например, общедомовые приборы учета имеются менее чем в 30% МКД. По поводу того, кто должен оплачивать установку таких приборов, до сих пор существуют разные мнения. Уровень оснащенности индивидуальными приборами учета варьируется от 50% для водоснабжения до 80% для электроснабжения. А доля приборов учета, способных передавать данные дистанционно, в жилом секторе ничтожно мала – менее 1% (см. таблицу).

Проведенный Т. Толмачевой анализ бухгалтерской отчетности игроков рынка в 2018 г. (данных за 2019 г. пока нет) показал, что работающие на рынке «умного» ЖКХ компании развивались неодинаково: у кого-то выручка падала, у кого-то стагнировала, и лишь единичные компании демонстрировали рост. Можно сказать, что рынок цифрового ЖКХ в 2018–2019 гг. практически не вырос. Почти 2/3 рынка приходится на сегмент автоматизированных систем коммерческого учета электроэнергии (АСКУЭ) (рис. 4), и по многим причинам превалирование этого сегмента сохранится в перспективе трех-пяти лет.

Коммунальные ресурсы	ХВС	ГВС	Электрическая энергия	Газ	Тепловая энергия	Сточные бытовые воды
Кол-во МКД, в которые поставляется ресурс, тыс.	867	487	1179	711	631	734
Доля МКД, оснащенных ОДПУ, %	28	24	34	0,4	33	0,4
Кол-во помещений МКД, в которые поставляется ресурс, тыс.	51 835	38 571	63 540	38 941	42 945	46 710
Оснащенность помещений МКД приборами учета, %	52,7	48,5	80	44	3	2

Источник: ГИС ЖКХ

◀ Уровень оснащенности жилого сектора приборами учета коммунальных ресурсов

Впереди операторы связи

В целом потенциал рынка цифрового ЖКХ велик – десятки миллионов домохозяйств, сотни тысяч коммерческих организаций. Есть за что бороться коммерческим организациям. И эта борьба уже началась, в том числе среди операторов связи.

Активен на рынке «Ростелеком». В 2019 г. крупнейший российский провайдер цифровых услуг в сотрудничестве с НПО «Карат» (Екатеринбург) развернул сеть для индивидуальных (ИПУ) и общедомовых приборов учета (ОДПУ) коммунальных ресурсов. В Новосибирской области совместно с компанией «Технотроникс» оператор установил систему удаленного сбора данных ОДПУ. В партнерстве с Департаментом информационных технологий г. Москвы организовал передачу телеметрических данных с коммунального транспорта, а с Министерством ЖКХ Московской области создал систему модернизации котельных.

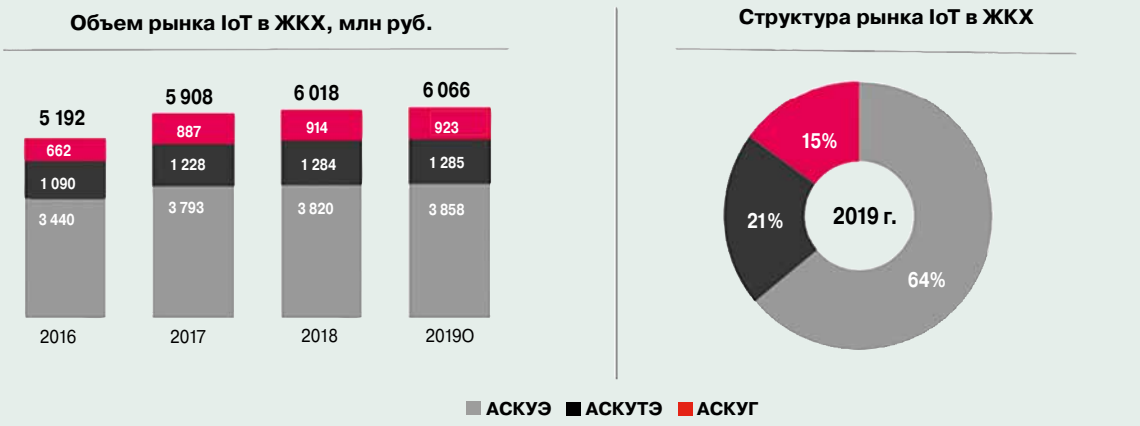
В апреле 2019 г. в Москве компании Tele2 и «Ростелеком» протестировали решения интернета вещей для ЖКХ в тестовой LTE-сети Tele2 с использованием технических решений Nokia и модемов со встроенными SIM-картами «Ростелекома». Показания счетчиков потребленной электроэнергии передавались на серверы энергосбытовых компаний. Инфраструктура позволила скомбинировать виртуализированное облачное пакетное ядро Nokia, ресурсы сетей радиодоступа Tele2 и транспортной сети «Ростелекома» с конечным оборудованием отечественных поставщиков.

В пилотной зоне использовалась технология NB-IoT, обеспечивающая возможность одновременного подключения сотен тысяч IoT-устройств. Сигнал сети NB-IoT хорошо проникает в труднодоступные места, такие как подвалы и подземные парковки, а технологии энергосбережения и малое энергопотребление дают устройствам возможность работать от одной батарейки в течение 10 лет. Аналогичные испытания компании Tele2 и «Ростелеком» провели в конце 2018 г. в сотрудничестве с Ericsson.

Компания МТС развернула систему автоматизации логистики вывоза мусора (АСУ «Управление отходами») и осуществила интеграцию своих систем с ГИС ЖКХ, Государственным кадастром недвижимости, системами ФНС, «Яндекса» и Google. Над системами управления зданиями и городским освещением, решениями в области энергомониторинга работает компания «ЭР-Телеком», «умным» ЖКХ занялись «Билайн» и «Мегафон».

Экосистема рынка

Особенность рынка цифрового ЖКХ – многочисленность его участников. Помимо операторов связи в находящуюся на стадии формирования экосистему входят производители приборов учета, автоматических систем для



◀ Рис. 4. Показатели развития рынка интеллектуальных измерений в ЖКХ

Источник: iKS-Consulting

▲ **Рис. 5. Экосистема «умного» ЖКХ**

ЖКХ, интеграторы, вендоры платформ и разработчики приложений (рис. 5).

Рассматривая участников экосистемы, стоит отметить холдинг «Росэлектроника» госкорпорации «Ростех», который планирует производство автоматизированных систем удаленного контроля потребления энергоресурсов для МКД. Создаваемая им система «СиТКоМ» находится на стадии конструкторско-испытательных разработок. Пилотный проект реализуется Рыбинским заводом приборостроения холдинга «Росэлектроника» совместно с компанией «Инсолар-Инвест».

Входящий в «Росэлектронику» холдинг «Швабе» разрабатывает «умные» приборы учета электроэнергии, цифровые комплексы для ситуационного управления городской инфраструктурой, в том числе энергоснабжением, оборудование для ЦОДов. Серийное производство «умных» счетчиков организует в 2020 г. входящее в холдинг «Росэлектроника» НПП «Исток» им. Шокина. Оценивает возможность производства приборов учета электроэнергии даже концерн «Калашников».

Среди городов в области «умного» ЖКХ лидирует Москва. Компания «Инспарк» запустила пилотный проект «Смарт-квартал» в Марьино. «Умный» квартал объединяет семь многоквартирных домов, в которых живут более 3 тыс. человек. Объединенная диспетчерская контролирует водоснабжение, подачу электроэнергии, центральное отопление, лифтовое хозяйство. На пульт диспетчерской информация поступает от систем видеонаблюдения и контроля доступа в помещения, от датчиков влажности и шума в подъездах, от противопожарных систем и домофонов. Решение проверяет уровень заполнения твердыми отходами шести площадок с «умными» контейнерами, управляет уличным освещением и электрозаправками. Благодаря работе системы оптимизируются затраты на обслуживание и ремонт коммунальных систем, снижаются расходы на электроэнергию, повышаются комфорт и безопасность городского пространства.

Вызовы 2020 года

В 2018–2019 гг. произошли три важных события в части реализации ведомственной программы «Умный город». Разработана и утверждена методика расчета «IQ» городов, разработан проект постановления правительства о финансовой поддержке субъектов Федерации при реализации программы «Умный город» и принят ФЗ-522, обязывающий сетевые и ресурсоснабжающие организации устанавливать «умные» электросчетчики за свой счет. Причем в случаях, когда прибора учета у потребителя нет, прибор вышел из строя либо его межповерочный интервал подошел к концу, закон должен применяться уже с 1 июля 2020 г. С 2022 года использование умных счетчиков должно стать обязательным. Все эти меры подстегнут развитие рынка интернета вещей для ЖКХ.

Однако пандемия коронавируса и карантинные мероприятия окажут на рынок негативное влияние. Направленные на развитие ИТ-бюджеты пока заморожены. Можно ожидать их сокращения, как и сокращения бюджетов госпрограмм. Из-за роста социальной напряженности в результате ухудшения экономической ситуации возможен перенос на более поздние сроки запланированного на июль вступления в силу закона ФЗ-522.

По оценке Т. Толмачевой, при оптимистичном сценарии рынок удержится на уровне 2019 г., при пессимистичном – упадет. Уровень падения будет зависеть от нескольких факторов, в том числе от объема секвестрования бюджетов на программу «Умный город» и сроков вступления в силу ФЗ-522. Действительно, пока не известно, когда закончится пандемия и какова будет глубина экономического кризиса, делать прогнозы относительно рынка «умного» ЖКХ крайне трудно. С уверенностью можно утверждать одно – конкурсная борьба за субсидии и гранты сильно обострится. ИКС

Импортозамещение в промышленности: на уровне софта, но не «железа»

Россия может преодолеть технологическое отставание в аппаратной сфере за счет ИТ и облачных сервисов, считает советник компании «УГМК-Телеком» Ильдар Гималтдинов.

Еще два года назад рынок ИТ в России составлял $3,07 млрд по данным IDC и $8–9,3 млрд по данным ассоциации «Руссофт» (с учетом SaaS и услуг внедрения). В 2019 г. российский рынок ИКТ, включающий телеком, производство оборудования, оптовую торговлю этим оборудованием и собственно ИТ, достиг, по данным IDC, $47,05 млрд, что стало наивысшим показателем в Центральной и Восточной Европе. Сейчас уже ясно, что даже осторожные прогнозы на рост ИТ-сектора в текущем году не сбудутся. Эксперты IDC ожидают падения ИТ-рынка в 2020 г. на 15–40% и связывают это с сервисным характером отрасли, обслуживающей другие сектора экономики и прямо зависящей от их бюджетов и планов развития. С другой стороны, именно угроза вынужденного простоя стимулирует промышленность активнее изучать, отбирать, внедрять инновации, необходимые для дистанционной работы. Если бэк-офис – от юристов и финансистов до проектного менеджмента и продаж – практически безболезненно перешел на «удаленку», то по поводу автоматизации производственного цикла как такового по-прежнему идут дискуссии.

– Ильдар, пандемия и карантинные меры возвращают нас к дискуссии об импортозамещении, которая стартовала шесть лет назад после введения антироссийских санкций. Как вы считаете, удалось ли достичь каких-либо результатов?

– Импортозамещение уже много лет остается актуальной задачей для России. После введения антироссийских санкций она вышла на первый план. В связи с пандемией, ограничениями экономической деятельности и предельным осложнением трансграничной логистики мы видим, насколько важно иметь собственные решения, но при этом бизнесу все еще приходится во многом полагаться на иностранных партнеров. Дело в том, что любая технология имеет две составляющие – аппаратную и программную. Российские разработчики сильны и признаны во всем мире. Их решения вполне могут конкурировать с зарубежными аналогами, а зачастую не имеют таковых. Наши программисты обеспечивают бизнесу современный и востребованный продукт.

В том, что касается аппаратных комплексов, мы существенно отстаем от передовых индустриальных стран. Чтобы создать ноу-хау в этой области, нужны долгосрочные, «тяжелые» инвестиции. Без них ни о каком импортозамещении и думать не стоит. Прежде чем выпустить аппарат на рынок, его нужно придумать, сделать прототип, провести испытания и моделирование работы в различных условиях эксплуатации. Для этого необходима сильная технологическая основа и научная база, требующая финансирования.

Если взять конкретно промышленность, то здесь самым перспективным направлением являются даже не ИТ, а IoT – интернет вещей. По прогнозам международных экспертов, уже в этом году между собой будет взаимодействовать более 50 трлн устройств – от бытового оборудования и смартфонов до станков, автономного транспорта и производственных роботов. Помимо «железа», т.е. компьютеров, сенсоров и датчиков, здесь большую роль играют технологии связи – различные системы и сети для стабильной передачи огромных потоков данных. К сожалению, в этой области Россия серьезно отстает от мировых лидеров – США, Китая и Южной Кореи. Возьмем данные

патентной аналитики за 2019 г. Так, в области IoT-решений для сельского хозяйства Россия даже не входит в первую двадцатку стран по количеству запатентованных решений. В традиционно сильном для нас секторе энергетики мы занимаем 24-е место с восемью заявками, в то время как у США их 4573, у Кореи – 2883, а у Китая – 263. В промышленном IoT результаты тоже не впечатляют: Россия находится на 35-м месте с тремя заявками. У США их более 5 тыс. Хотя патенты и не идеальный показатель, но расти нам, безусловно, есть куда.

– Изменила ли ситуацию пандемия коронавируса? Сейчас много говорят о том, что необходимость соблюдать карантинные меры подталкивает предприятия активнее внедрять передовые технологии, обеспечивающие возможность удаленной работы, – вплоть до роботизированных комплексов, благодаря которым производство становится полностью безлюдным.

– Пандемия показала, насколько промышленность нуждается в инновациях для реализации программ Индустрии 4.0. Например, относительно понятная технология цифровых двойников используется в единичных компаниях. Так, госкорпорация «Ростех» активно применяет ее в двигателестроении, в «Газпром нефти» ее внедрением занимаются на перерабатывающих производствах. Использование технологии нельзя назвать массовым – по крайней мере в России. Сейчас все с большим интересом ждут результатов реализованных проектов. Только тогда бизнес поймет, что инновационные решения действительно работают. Тем не менее, по прогнозам экспертов, через пять лет этот рынок достигнет $16 млрд.

Что касается роботизированных производственных комплексов, не стоит рассчитывать, что в краткосрочной перспективе машины смогут заменить основной персонал, занятый, к примеру, на добыче руды, дальнейшей переработке породы в полуфабрикат, концентраты и т.д. Сегодня полноценно трудиться в удаленном режиме могут только инженеры технических служб. Однако необходимы средства коммуникации между ними и теми работниками, которые остаются непосредственно на промышленной площадке.

> Четвертая промышленная революция требует определенной перестройки сознания. Сегодня многие крупные предприятия имеют целые департаменты цифровой трансформации. Однако значительная часть промышленного менеджмента относится к подобным решениям скептически.

– С какими сложностями сопряжена подобная автоматизация?

– В промышленности многие говорят, что роботов стоит использовать на площадках, создаваемых с нуля. Думаю, это верный подход. Сложность заключается в перестройке производственных цепочек. Нужны новые корпуса, склады, стеллажи, разнообразные конструктивные переделки, и все это стоит дорого. А вот новые площадки вполне можно создавать, изначально учитывая, что они будут в значительной степени роботизированы.

– Часто высказываются опасения, что в перспективе роботы вытеснят с рынка труда людей. Насколько оправданы подобные ожидания? Может ли автоматизация привести к негативным социальным последствиям?

– Автоматизация – единственный способ конкурировать с ведущими российскими и мировыми компаниями. В долгосрочной перспективе нас, несомненно, ждет полная роботизация производственного цикла. Что касается персонала, который рискует остаться без работы на фоне этих процессов, государство и компании должны уже сегодня задуматься о том, как они будут спасать рынок труда, помогая людям диверсифицировать свои навыки, развивать soft skills, получать новую востребованную профессию. У нас и сейчас есть много «недоукомплектованных» профессиональных областей. А вообще, уверен, что тех же ИТ-специалистов можно переучивать в любом возрасте. Чем больше людей будет работать в этой сфере, тем быстрее мы станем ведущей ИТ-державой.

На производстве же роботы будут более эффективны, полезны и продуктивны по сравнению с людьми. Как минимум они не болеют, не курят и работают 24 часа в сутки. Качество, производительность, отсутствие эксцессов, связанных с охраной труда и безопасностью производства, – список плюсов можно продолжать.

– Какие решения в сфере автоматизации востребованы уже сегодня?

– Прямо сейчас предприятия решают локальные и оперативные вопросы. Это все, что касается загрузки мощностей, – на день, неделю,

месяц. Кроме того, необходимо отслеживать всю технологическую цепочку с точки зрения качества изделий и заготовок. И здесь оказались чрезвычайно востребованы разнообразные системы видеонаблюдения. Эти комплексы также помогают удаленно инвентаризировать оборудование цехов. Актуальны тепловизоры, разнообразные системы, позволяющие наблюдать за сотрудниками, контролировать ситуацию в цехах. В России такие технологии есть, и некоторые из них перспективны. Но важно, чтобы бизнес мог оценить их эффективность. Пока под рукой есть человек, бизнесу проще. Человек расскажет, нарисует, убедит и т.д. Верят именно живой голове.

– Это просто экономия усилий? Нежелание развиваться, если все и так работает?

– Это во многом вопрос мировоззрения. Четвертая промышленная революция требует определенной перестройки сознания. Сегодня многие крупные предприятия имеют целые департаменты цифровой трансформации, призванные помочь преодолеть пресловутый цифровой разрыв и приблизить новый технологический уклад. Однако значительная часть промышленного менеджмента относится к подобным решениям скептически.

– Как автоматизация производственных и бизнес-процессов сказывается на информационной безопасности предприятия?

– Разумеется, в условиях автоматизации эти вопросы приходится решать на новом уровне. Когда значительная часть процессов переносится в облака, необходимо держать большой штат сотрудников, которые представляют себе, какую систему мы, собственно, защищаем. Несмотря на наличие нескольких громких брендов, специалистов по информационной безопасности на российском рынке мало. Это приводит к тому, что в промышленности системы безопасности защищают не весь комплекс рабочих ресурсов, а только отдельные участки. Это забор, который в одних местах высокий, крепкий и непреодолимый, а в других – хилый и шаткий. Как правило, на одном предприятии установлено несколько систем безопасности, плохо взаимодействующих между собой.

Сейчас, когда из-за карантина многие сотрудники начали работать из дома, появилась дополнительная задача – защитить канал, по которому они обращаются к рабочим сервисам с личных компьютеров. Такие облачные платформы, как Amazon Web Services или Microsoft Azure, до недавнего времени использовавшиеся компанией Zoom в качестве провайдеров, изначально не были предназначены для того, чтобы к ним обращалось так много людей, и потому они временами попросту не выдерживают нагрузки. Это создает дополнительные уязвимости, которыми могут воспользоваться хакеры.

> В долгосрочной перспективе нас ждет полная роботизация производственного цикла. Что касается персонала, который рискует остаться без работы на фоне этих процессов, государство и компании должны уже сегодня задуматься о том, как они будут спасать рынок труда, помогая людям диверсифицировать свои навыки, получать новую востребованную профессию.

– Каким, на ваш взгляд, должен быть механизм внедрения инноваций в промышленности? Какие институты могут способствовать этому процессу?

– Уверен, один из эффективных инструментов, помогающих промышленности минимизировать риски и внедрить действительно нужные и эффективные инновационные решения, – это программы отбора и поддержки высокотехнологичных проектов. Дело в том, что они помогают «держать нос по ветру», отслеживать все новое и подбирать то, что нужно конкретной компании. Часто крупный промышленный бизнес боится работать с технологическими стартапами, а такие программы дают ему возможность просчитать все риски и принять взвешенное решение о сотрудничестве, заключить сделку, запустить пилот. В результате мы можем видеть колоссальный эффект в плане продвижения ИТ в нашей стране. К примеру, в марте этого года программу, ориентированную на поиск эффективных решений, которые способны модернизировать российскую промышленность, запустили Фонд «Сколково» и Инновационный центр «Ай-Теко».

Возвращаясь к тому, с чего я начал, подчеркну, что Россия может преодолеть технологическое отставание в аппаратной области как раз за счет ИТ и облачных сервисов. Программные решения позволят нам избежать прямого производства «железной» компонентной базы, т.е. вообще не играть на том поле, на котором мы исторически не очень сильны. ИКС

5 типичных ошибок при импортозамещении

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

Переход к использованию импортозамещающих продуктов в российском госсекторе – процесс небыстрый и не всегда простой. Мы выделили пять типичных ошибок, которые помешают вам выполнить требования регуляторов и заставят проделать двойную работу.

1 Переход на продукты, не включенные в реестр отечественного ПО

Часто в попытке сэкономить государственные организации внедряют программное обеспечение, не включенное в Единый реестр российских программ для ЭВМ и баз данных. При этом ряд приказов, изданных Минкомсвязью России, прямо указывает на недопустимость таких приобретений.

Многие компании стремятся осуществить переход с популярных импортных офисных программ – редакторов таблиц, текстов и презентаций – на продукт, относящийся к свободному программному обеспечению (СПО). Таким образом они надеются достичь нужных показателей импортозамещения и сэкономить средства. Конечно, бесплатность – важное преимущество СПО. Однако оно не будет учтено при подсчете показателей импортозамещения, поскольку не включено в реестр. Работу придется начинать заново. Представьте, сотрудники уже научились пользоваться установленным СПО, продукт интегрирован с развернутыми в организации информационными системами, оформлен ряд внутренних нормативных документов, регламентирующих эксплуатацию данного решения. И вся эта трудоемкая работа окажется напрасной.

Бывает, что виновник ошибки не сам заказчик, а разработчик, продукт которого внедряется. Нередки случаи, когда вендоры обещают заказчику, что их продукты в ближайшее время попадут в реестр отечественного ПО. Но, как показывает практика, процесс может быть длительным. Особенно важно обратить внимание на эту деталь, если поставщик софта определяется в рамках тендера. В таком случае продукт должен входить в реестр уже на момент проведения тендерных процедур. Если же вы покупаете ПО без тендерной процедуры, оно вам подходит и разработчик уверяет, что продукт вот-вот появится в списке рекомендуемых, проверьте статус заявки на сайте реестра.

2 Ожидание конца срока действующих лицензий

Многие руководители уверены, что наличие действующих лицензий на оборудованные рабочие места освобождает от перехода на отечественное ПО. Они считают, что замена должна быть плановой и осуществляться только после окончания срока действия старой лицензии. Эта ошибка связана с психологической неготовностью руководителей оперативно принимать нужные решения. На самом деле законодательство РФ обязывает перейти на отечественный софт все федеральные, региональные, муниципальные органы и подведомственные им организации вне зависимости от наличия ранее закупленных лицензий.

Заказчикам следует учитывать, что переход на новое ПО – процесс небыстрый, включающий несколько стадий, каждая из которых требует отдельного согласования. Чем раньше он будет запущен, тем более плавным и постепенным будет переход, и организация последовательно выполнит свои показатели импортозамещения.

3 Откладывание на потом

«У нас еще куча времени, успеем» или «мы все равно уже опоздали, так зачем спешить» – это ошибки одного ряда. Как правило, подобные заблуждения связаны с субъективными оценками сроков внедрения нового ПО руководителя-

ми организаций и их окружением. Есть примеры, когда президенту России приходилось лично указывать руководству некоторых крупных компаний на недостаточные темпы внедрения отечественных технологий. Опыт Softline показывает, что конструктивный диалог с анализом существующих в учреждении процессов и составление четкого графика перехода на российское ПО снимает все возражения. Помните, что скорость изменений зависит от скорости принятия решений. Откладывая на потом, вы значительно усложняете процесс перехода, так как теряете драгоценное время.

4 Несвоевременное обучение персонала

Кроме того, переход на новый софт сопряжен с бóльшим объемом работ и некоторыми рисками. Возрастает роль и загруженность директоров по информационным технологиям. От их компетенций и уверенности в собственных силах зависит, насколько быстро и безболезненно будет реализован проект импортозамещения. Игнорирование сложностей не выход из ситуации.

Отмечу, что в российских нормативных документах, регламентирующих процесс импортозамещения, говорится не о приобретении, а о преимущественном использовании отечественных решений. Главное не купить, а пользоваться! На этом этапе нередко возникает новая проблема, связанная с неумением персонала работать на отечественном ПО. Иногда эта проблема усугубляется уверенностью некоторых руководителей в принципиальной необучаемости своих подчиненных. Они ссылаются на возраст основного контингента сотрудников и т.п. Другие руководители считают, что сотрудники освоят новые продукты во время работы самостоятельно.

Получается странная ситуация: отечественное решение внедряется, а работать с ним никто не умеет. При этом значительно повышается порог сложности, что серьезно сказывается на тестировании – первом этапе перехода, который требует привлечения как технических специалистов организации, так и пользователей. Часто они не читают приложенные инструкции и ищут в новом ПО алгоритмы, к которым привыкли, работая со старыми системами. Это сильно затрудняет им процесс адаптации к отечественному софту. И виноват в этом не персонал, а руководство, которое не уделило должного внимания обучению своих работников.

Важно провести обучение до внедрения новых продуктов хотя бы на уровне представителей ИТ-департамента, которые потом покажут остальным, как работать с новым ПО.

5 Заблуждения относительно применимости российских продуктов

Пятая распространенная ошибка – убежденность в несовместимости отечественного софта с продуктами безопасности или другим ПО, используемым в организации. Некоторые руководители утверждают, что в российских решениях им не хватает функционала. В большинстве случаев это заблуждение или отговорка. Здесь нужно смотреть на необходимый и достаточный функционал. Часто избыточные возможности, которые есть в зарубежных аналогах, большинству сотрудников не нужны. Для обычного пользователя важно, чтобы стабильно работали те приложения, к которым он обращается ежедневно.

Проблемы совместимости российского ПО с другими отечественными продуктами действительно имели место на заре перехода к импортонезависимости. К настоящему времени ситуация изменилась, и вендоры активно работают над совместимостью своих решений с популярными решениями других разработчиков.

В вопросах безопасности отечественного софта сегодня также достигнут большой прогресс. Российские операционные системы Astra Linux, «Альт», РЕД ОС совместимы с отечественными средствами криптографической защиты – «КриптоПро» и программным комплексом VipNet, что подтверждено сертификатами. Специальные требования к уровню защиты информации часто прописаны в условиях проведения тендеров на поставку ИТ-продуктов для госорганизаций. Широкий спектр продуктов, с которыми работают госорганы, предполагает, что вопросы безопасности всегда находятся в приоритете. И заниматься ими должны именно отечественные специалисты.

Говорят, что ошибок не совершает тот, кто ничего не делает, но, когда речь идет о таком непростом процессе, как выбор ПО для бесперебойного функционирования организации, лучше минимизировать возможность их возникновения. Сделать это можно, вовремя обратившись к компетентным ИТ-компаниям, специалисты которых имеют достаточную экспертизу во внедрении российского софта. Так вы сможете сэкономить время, нервы и средства предприятия и своевременно выполнить требования законодательства. ИКС

Карта рисков: что, зачем и как

Антон Грецкий, специалист по безопасности, ActiveCloud

Карта рисков – простой и наглядный инструмент, который позволяет классифицировать риски по степени критичности для бизнеса и оценить общее состояние риск-менеджмента в компании. Однако принимать ключевые решения, опираясь только на нее, не следует.

Многим компаниям, ведущим бизнес с использованием информационных технологий, необходимо подтверждать, что сами эти технологии и данные надежно защищены. От этого зависят репутация бизнеса, доверие клиентов и стабильное положение на рынке. Современные стандарты информационной безопасности, такие как COSO, ISO 31000: 2009, ISO/IEC 27005: 2011, большое значение придают риск-менеджменту, поскольку он, помимо прочего, является важным аспектом контроля со стороны национальных регуляторов. Популярный инструмент определения и ранжирования рисков – карта рисков.

Рис. 1. Форма карты рисков ▼

Вероятность, баллы	**Ущерб**, баллы				
	Крайне низкий, 1	Низкий, 2	Средний, 3	Высокий, 4	Крайне высокий, 5
Крайне низкая, 1					
Низкая, 2					
Средняя, 3					
Высокая, 4					
Крайне высокая, 5					

Оценка рисков как основа безопасности бизнеса

Оценка рисков – важный шаг для каждой компании, направленный на минимизацию потерь. Важно определить, какие риски внутри компании и во внешней среде для вас существенны, а какими можно пренебречь.

Карта рисков – инструмент, который позволяет классифицировать риски по степени критичности для бизнеса. Кроме того, она поможет понять, какие риски бизнес может принять, не обрабатывая.

Наличие актуальной карты рисков свидетельствует о том, что риски идентифицируются, анализируются и обрабатываются. Ее можно демонстрировать проверяющим регуляторам, рейтинговым агентствам, банкам, акционерам в качестве подтверждения действующей системы риск-менеджмента в вашей компании.

Как создать карту рисков?

Исходные данные для составления карты рисков – реестр, включающий все риски, присущие вашему бизнесу, и форма карты (рис. 1) для ее наполнения выявленными рисками. В процедуре наполнения карты должны участвовать владельцы технических и бизнес-процессов, чьи риски будут оцениваться.

Оценку каждого риска в карте будем проводить по двум параметрам/шкалам – вероятность реализации и потенциальный ущерб. В качестве градаций обычно выбирают «низкий», «высокий» и «средний» уровень. Для более точного позиционирования рисков в карте можно разделить верхнюю и нижнюю границы, добавив значения «крайне низкий» и «крайне высокий» (критический). Уровню «крайне низкий» присваиваем значение 1, «низкий» – 2, «средний» – 3, «высокий» – 4 и «крайне высокий» – 5.

Оценка ущерба. Ущерб, в результате которого работа вашего бизнеса окажется под угрозой, принимаем как «высокий»/«крайне высокий», низкий ущерб не подразумевает каких-либо последствий для бизнеса.

Оценка вероятности. Высокая вероятность риска может означать, что подобные риски в прошлом уже неоднократно реализовывались или что риск, судя по некоторым признакам, вот-вот реализуется. Вероятность можно считать низкой, когда риск не реализовывался уже несколько лет и предпосылок к этому не предвидится.

Относительное значение уровня риска – это произведение двух величин: вероятности реализации риска и ущерба от этого. Таким образом, минимальное относительное значение уровня риска будет равняться 1 – вероятность крайне низка (1) и ущерб также крайне низок (1). Максимальное относительное значение риска равно 25 – когда и уровень ущерба, и вероятность его реализации крайне высоки (рис. 2). Все риски компании будут ранжироваться в этом диапазоне, от 1 до 25.

Сгруппируем риски для дальнейшей работы:

- диапазон 1–2 относительного значения риска будем считать крайне низким, такие риски можно принять без компенсационных мер;
- диапазон 3–5 соответствует низким рискам, обрабатывать которые можно в последнюю очередь;
- 6–15 – средние риски;
- 16–20 – высокие риски;
- 25 – крайне высокие риски, обработка которых является первоочередной задачей.

Как использовать карту рисков?

Карта рисков, безусловно, полезна, однако при принятии ключевых решений в сфере инвестирования, формирования стратегии, утверждения бюджетов, разработки планов развития и т.п. не следует опираться только на нее. Дело в том, что карта рисков по своей природе – инструмент неточный и оценочный. Она описывает одной точкой неопределенность, которая имеет огромное количество сценариев, не учитывая при этом вариации и распределения.

Вероятность, баллы	**Ущерб**, баллы				
	Крайне низкий, 1	Низкий, 2	Средний, 3	Высокий, 4	Крайне высокий, 5
Крайне низкая, 1	1	2	3	4	5
Низкая, 2	2	4	6	8	10
Средняя, 3	3	6	9	12	15
Высокая, 4	4	8	12	16	20
Крайне высокая, 5	5	10	15	20	25

▲ **Рис. 2. Карта с цветовой дифференциацией рисков**

Многие эксперты в области риск-менеджмента указывают, что использование этого инструмента для принятия решений само является рискованным. Например, авторы исследования «Риск использования карты рисков»* указывают, что карты рисков классифицируют значения ущерба и вероятностей, однако не существует устоявшихся правил, как выполнять классификацию. Ранжирование, производимое риск-менеджером, зависит от произвольного выбора, и этот произвольный выбор часто дает произвольный результат.

Большинство компаний в мире (за исключением постсоветского пространства) перестали всерьез заниматься картами рисков, заменив их другими инструментами принятия решений. В качестве альтернатив можно выбрать имитационное моделирование, сценарный анализ, анализ чувствительности, деревья решений.

Карта рисков хорошо подходит для презентации процедур риск-менеджмента в компании. Она способна отразить «в крупную клетку» общее состояние управления рисками. Это действительно удобный и понятный графический способ подачи информации руководству компании, акционерам, регуляторам. Если преобладают желтая и зеленая зоны – ситуация под контролем, если красная и оранжевая – значит, управление рисками нужно срочно совершенствовать. Однако не полагайтесь на карту рисков для принятий стратегически важных решений, потому что она для этого не предназначена. ИКС

* P. Thomas, R.B. Bratvold, J.E. Bickel. The Risk of Using Risk Matrices. www.researchgate.net/publication/266666768_The_Risk_of_Using_Risk_Matrices

ЦОД не роскошь, а инструмент бизнеса

Дата-центры становятся рыночным продуктом, а приход на этот рынок крупных девелоперов даст мощный толчок развитию и может кардинально его изменить, считает Евгений Вирцер, генеральный директор компании «Свободные Технологии Инжиниринг».

Команда Евгения Вирцера хорошо известна на российском рынке цодостроения. Создав собственную компанию – «Свободные Технологии Инжиниринг», – они начали работать де-юре с чистого листа. Но с большим опытом реализованных проектов.

– Евгений, какие, по вашим наблюдениям, произошли значимые изменения в области цодостроения за последние 10 лет?

– Сегодня ЦОД уже не роскошь, а инструмент бизнеса. Как следствие, он становится рыночным продуктом, появляется технологическая конкуренция. При этом нужно учитывать, что стоимость стойко-места не растет, а в некоторых случаях уменьшается, но цена основного инженерного оборудования увеличивается постоянно. Чтобы успешно работать в условиях таких «ножниц», надо использовать более открытые и совершенные технологии. Но тут есть сложности.

Нередко возникают ситуации, когда люди начинают строить ЦОД в неоптимальных, мягко говоря, условиях. Например, купили здание, которое изначально для ЦОДа не предназначалось. Приходится вписывать инфраструктуру ЦОДа в существующие конструкции. В результате решения получаются более сложными и дорогими. А можно было снести купленное здание, построить на его месте новое, спроектированное под ЦОД, и объект получился бы лучше и дешевле. Чем меньше ограничивающих факторов, тем больше возможностей использовать более совершенные технологии и построить идеальный ЦОД.

Еще один важный момент связан с тем, что все стали обращать внимание на энергоэффективность. PUE и другие подобные показатели – на первой странице любого ТЗ. 10 лет назад никто за редким исключением на PUE не смотрел. Это, конечно, не значит, что сегодня заказчики автоматически выбирают максимально энергоэффективные решения. Но они уже анализируют расклад между CAPEX и OPEX, оценивают общую стоимость владения.

Знаковая тенденция – растущий интерес к теме ЦОДов со стороны девелоперов. Их системный выход на рынок может если не перевернуть его целиком, то точно оказать на него сильное влияние. Мы уже принимаем активное участие в проектировании ряда таких объектов, причем очень масштабных. Один из них – ISTRADIGITAL, где в рамках первого в России многофункционального технологического центра планируется построить ЦОДы общей емкостью 40 тыс. стоек. Другой проект, реализуемый опытным девелопером в области индустриальной недвижимости, предполагает создание на севере Москвы ЦОДа на 5,5 тыс. стоек.

– Какой вы видите роль девелоперов на рынке ЦОДов?

– По большому счету ЦОД – такой же объект недвижимости, как жилой комплекс, бизнес-центр или склад. В чем-то он сложнее, а в чем-то – даже проще. Девелоперы строят ЦОД, а потом либо продают оператору, либо сдают в долгосрочную аренду.

В США, например, рынок строительства коммерческих дата-центров – по большей части рынок девелоперов. У нас это рынок операторов, для которых строительство ЦОДов – обязательное условие ведения основного бизнеса. А для девелоперов строительство ЦОДов и есть основной бизнес. Они профессионалы в строительстве: гораздо более эффективно умеют получать площадки, подводить туда электрические мощности, строить. Операторы строят редко, поэтому, что бы они ни говорили, они не могут быть самыми эффективными в этом деле. Плюс ко всему у девелоперов выстроена схема с финансированием проектов строительства, тогда как для оператора найти деньги на новый объект – задача непростая.

Девелоперы не собираются конкурировать с операторами ЦОДов, они хотят, чтобы те стали их клиентами. Думаю, девять из десяти операторов с радостью зайдут на готовый объект, в котором отсутствуют CAPEX, – спокойно плати аренду и зарабатывай деньги на своих сервисах.

Повторю, приход крупных девелоперов на рынок ЦОДов даст мощный толчок его развитию. Прирост числа стоек будет происходить гораздо более быстрыми темпами, чем сейчас.

– Процессы на рынке значительно ускорились. Заказчики уже не могут ждать нового ЦОДа два-три года. Что позволяет повысить скорость проектирования и строительства таких объектов?

– Любые инвестиции требуют максимально быстрого начала их возврата. Арифметика простая: построили ЦОД за год, инвестиции начали возвращаться через год, построили за два года – через два и т.д. Да и построенный за два года объект будет дороже такого же объекта, построенного за год, ведь ресурсы заказчика, интегратора и других участников проекта будут расходоваться в течение вдвое большего периода времени.

Рецепты ускорения реализации проектов хорошо известны – это использование модульных, типовых решений, в том числе с высокой степенью заводской готовности (такие решения часто называют префабами. – *Прим. ред.*). Мы уже активно применяем подобные решения, будем задействовать их еще шире. Плюсы – отличная масштабируемость, высокая скорость выполнения работ, минимизация числа чувствительных к качеству процессов на стройплощадке. Минус – цена, но при более высокой стоимости отдельных элементов общая стоимость объекта может быть существенно ниже. Экономия достигается за счет сокращения операций на площадке – это основной путь к повышению эффективности и качества строительства.

Наша мечта – минимизировать количество людей на площадке строительства. ЦОД – инженерно насыщенный объект, плотность инженерных систем, число пересечений коммуникаций высочайшие. Часто на площадку одновременно выходят электрики, кондиционерщики, пожарники, топчутся на одном месте, мешают друг другу. Возникают проблемы с качеством, срываются сроки. При строительстве ЦОДа из готовых «кубиков» таких сложностей нет.

В качестве примера приведу ЦОД Сбербанка в Сколково, в реализации которого участвовала наша команда. Сроки были сжатые. Поэтому было решено изготавливать коридорные модули (6 х 3 х 3 м) не на площадке, как это обычно делается, а в заводских условиях – параллельно с выполнением строительных работ. Монтаж коммуникаций в модуле проводился в производственном цехе, что повышало качество. Установка готовых модулей на площадке происходила в 10 раз быстрее, чем создание таких же элементов в «полевых условиях». Мы будем стараться использовать эту практику и на новых объектах.

– И все же: как быстро сегодня можно построить крупный ЦОД?

– Скорость реализации сильно зависит от организационных факторов. Скажу так: с момента согласования всех технических моментов с заказчиком, при наличии готовой площадки и финансирования, ЦОД на 2 тыс. стоек можно сделать под ключ за 12 месяцев. Это задача непростая, но выполнимая.

Один из важных моментов, как и в любом сложном деле, – правильный подбор команды. Как уже говорил, ЦОД – насыщенный взаимоувязанными инженерными системами объект. Понятно, что любой технически грамотный и опытный в сфере проектирования и строительства технологических зданий подрядчик сможет спроектировать и построить ЦОД. Другой вопрос, насколько быстро и успешно он справится со всей спецификой, часто спрятанной в мелочах.

– Наверное, сократить сроки реализации проекта позволяют цифровые технологии, например BIM?

– Считаю, что в проектах ЦОДов без BIM уже нельзя. По сути, создается цифровой двойник ЦОДа. BIM-модель построенного объекта включает в себя исполнительные чертежи, схемы, паспорта оборудования, сертификаты и прочие знания, накопленные в ходе строительства. Это помогает службе эксплуатации управлять объектом и пользоваться данными о нем. В одном из проектов мы интегрировали цифровой двойник в систему управления зданием и систему управления эксплуатацией. В будущем есть планы настроить систему обучения и подготовки кадров с применением технологий виртуальной и дополненной реальности.

– Последние год-два заметно оживился региональный рынок. В чем специфика создания ЦОДов в регионах? Хватает ли высококвалифицированного персонала?

– Основные проблемы во многих регионах – невысокий уровень развития телекоммуникационной инфраструктуры, а также отсутствие якорных заказчиков, готовых хранить большие объемы данных в коммерческих ЦОДах.

Еще один важный момент – особенности культуры хранения и обработки данных. Многие компании только начинают осознавать, что передача ИТ-ресурсов и сервисов на аутсорсинг не несет дополнительных рисков для предприятия, а наоборот, повышает устойчивость информационных систем. У большинства компаний психология пока на уровне «если я кому-то отдам свои данные, то их или сворują, или потеряют», отсюда бесчисленное количество нелепых серверных в местах, которые для этого не предназначены.

Чтобы в регионах оперативно перейти от слов к делу, все-таки сначала должны появиться качественные ЦОДы, пусть небольшие. Заказчики «руками и глазами» почувствуют, что это удобно, комфортно и безопасно. А что касается персонала – у нас есть регионы с высоким уровнем технических компетенций. Хотя кадровая проблема существует везде, даже Москва не исключение. Опять же модульность и однотипность решений дают возможность сгладить эти сложности.

– Не могу не спросить про влияние пандемии на рынок ЦОДов.

– Большинство компаний, специализирующихся на предоставлении ИТ-сервисов, растут вместе с повышением спроса на «цифру». Понятно, что местами этот рост носит спекулятивный характер, но он есть и, на мой взгляд, будет продолжаться. Конечно, как в любой кризис, надо аккуратнее подходить к оценке платежеспособности заказчиков – денег на рынке становится меньше. Но индустрия ЦОДов точно не относится к пострадавшим отраслям – это не туризм и не ресторанный бизнес.

Если говорить о нашей компании, то нынешнюю ситуацию, как и любой кризис, мы расцениваем как возможность для роста. Мы не закрывались на время пандемии, не считая перехода на две недели в онлайн, поэтому всегда были рядом с нашими партнерами и заказчиками, связь не прерывалась. Оптимизм внушает и постоянно увеличивающееся число проектов с нашим участием.

Классовая теория цифровой экономики

Не знаю, может быть, я тоже виноват. Или мы просто обуржуазились. А? Только с чего бы? И буржуазность-то наша какая-то дремучая, азиатская. Вроде не накопители. У меня вон один костюм, в котором выйти можно. Частной собственности нет, благосостояние растет. Ничего понять нельзя.
А. Тарковский. Сценарий к/ф «Зеркало»

Игорь Бакланов

Цифровая экономика – это новая индустриализация, и выполнять программу такой индустриализации можно только централизованно и только под руководством государства.

Наше время – время Карла Маркса. Предсказанный им крах капитализма, призраки, бродящие по Европе, революции – локомотивы истории... Пора вспомнить о классовой теории и законах капитализма и социализма. Мы – не просто первая страна, которая построила социалистическую экономику. Мы еще и первая страна, которая ее полностью разрушила, показав всему миру и своему народу в первую очередь весь блеск и нищету капитализма.

Соревнование двух систем

То, что раньше рассказывалось на политинформации в советской средней школе относительно «звериного оскала капитализма», вошло в нашу жизнь в полной мере: олигархия, коррупция, безработица, неэффективность управления в условиях рынка, лоббизм и совершенная невозможность решить «всем миром» какую бы то ни было проблему. Именно об этом писал в свое время забываемый ныне Игорь Шафаревич в работе «Две дороги – к одному обрыву». В ней он не просто по-диссидентски критиковал социализм, он показывал еще кое-что: капитализм ведет к тому же обвалу. Сделав ставку на индивидуализм, конкуренцию, рынок, неравенство, примат личного над общественным и священный характер частной собственности, капитализм не способен решить ни одной глобальной задачи. Он не может выиграть мировую войну ценой подвига, не может в короткие сроки создать современную экономику и науку, не способен справиться с глобальным потеплением и не поможет мобилизоваться в условиях вирусной пандемии – все это противоречит его основам. Капитализм хорош, когда снаружи все спокойно и можно комфортно, без рывков и с избыточными ресурсами обустроить жизнь. С играми в демократию, с медленной стабилизацией различных сторон жизни «невидимой рукой рынка». А современный мир требует решения именно глобальных задач. Это понимает уже каждый житель нашей страны, сидящий в изоляции в собственной квартире, доме или на даче.

У нас есть некоторое преимущество – значительная часть населения жила при социализме и может не понаслышке судить о достоинствах и недостатках двух принципов построения общества и понимать, откуда берутся те или иные явления в нашей жизни.

Построив и разрушив социализм, пытаясь закатать в асфальт и забыть собственный национальный опыт государственного строительства, наша страна получила некую раздвоенность в экономике – у нас присутствуют и социалистические, и капиталистические черты. С одной стороны, вот уже более тридцати лет в головы нашему народу заливают идеи капитализма. С другой стороны, куда девать масштабность русской души? Куда девать ощущение общего пути? Исторической значимости? Остатки нашего

патриотизма прочно базируются на советских идеях: народ-победитель, народ – носитель уникальной культуры, народ – покоритель космоса. Капитализм требует иного: космополитизма, либеральных ценностей, глобализации. И все это смешивается на всех уровнях: от московской кухни до законодательных актов.

Индустриализация vs капитализм

Взять, например, новую научно-техническую революцию – переход к цифровой экономике. Это глобальная перестройка экономики, перевод ее на новый уклад, новая индустриализация страны. Задача более чем масштабная, требующая мобилизации всех сил общества, центрального руководства, сильного государства, нового Госплана и нового ГОЭЛРО. Наша страна за XX век трижды (!) решала эту задачу: сначала индустриализация до 1913 г., затем сталинская индустриализация и индустриализация послевоенная, восстановление промышленности из руин после Великой Отечественной войны в течение 8–12 лет до запуска первого спутника и далее по пути планового развития.

Но все три индустриализации осуществлялись не в условиях капитализма. В царской России капитализм только начинал свое развитие, и это развитие привело к Февральской революции и развалу всей государственной машины на несколько десятилетий. А индустриализация России в конце 1920-х – 1930-х гг. проводилась социалистическим государством, т.е. централизованно. ГОЭЛРО как план индустриализации был разработан еще в начале XX века в рамках госзаказа на стратегию модернизации промышленности. Большевики только доработали его с учетом текущего исторического и политического момента. Так что нет в истории России опыта индустриализации в условиях капиталистических отношений.

Классовые противоречия, противостояние двух систем: социализма как метода проведения централизованной политики и капитализма как декларируемой властью системы общественных отношений – основа противоречий современной истории, экономики, политики, всех сторон жизни.

Цифровизация vs коммерциализация

Вернемся к программе цифровой экономики. Новый экономический уклад требует внедрения технологий Big Data, искусственного интеллекта, информатизации всех сфер промышленности и управления государством. В условиях планового хозяйства это была бы естественная стратегия, направленная на совершенствование управления экономикой. В условиях частной собственности новые технологии становятся гордиевым узлом конфликтов участников рынка и самого рынка. Капиталистическая эффективность требует не новых технологий, а максимальной прибыли и, как следствие, минимальных инвестиций в прогресс. Там, где прогрессор и инноватор прозревают будущее, капиталист видит бюджеты, подлежащие освоению, и прибыли, которые нужно сохранить и положить на депозит. Эта экономия никак не связана с результатами инноваций, поскольку капиталиста интересует только капитал, только финансовая сторона вопроса. В результате возникает явление «робких инноваций», когда инвестор дает деньги на разработку, но сразу же требует окупаемости и прибыли. Даже если инвестор – государство.

Глобальный конфликт между двумя экономическими формациями накладывается на сумбур в государственном управлении, в котором уживаются капиталистические и социалистические элементы. Такое сочетание иногда называют государственным капитализмом, а это понятие само по себе спорное.

Все программы инноваций, федеральные целевые программы импортозамещения, инновационные кластеры и пр. неизбежно попадают в зубчатые колеса противоречий двух формаций. Во всех инновационных программах присутствует термин «коммерциализация» – самый противоречивый термин в условиях НТР. Деньги даются только с возвратом, только при условии прибыльности, причем в очень короткий промежуток времени, период коммерциализации. Современные инженер и ученый обязаны думать даже не об экономике своей деятельности, а об ЭКОНОМИИ. Чтобы дебит с кредитом сошелся, чтобы каждая идея принесла прибыль. Это основа капитализма. Но она противоречит прогрессу. Можно ли построить ракетную промышленность, имея целью максимизацию прибыли? Да, можно, но не далее систем залпового огня «Катюша», которые востребованы на рынке. А искусственный спутник рынку не нужен. И первый человек в космосе – это не про прибыль. Вот и получается, что современная наука развивается там, где капитализм уже преобразуется в какие-то новые формы и формула

«деньги – товар – деньги» не имеет доминирующего значения. В странах «развитого Запада» есть свои механизмы инноваций – с фондами, инвесторами, биржами, IPO, бизнес-ангелами, акселераторами и пр. Но до этого прошло более ста лет «дикого капитализма». У нас же капитализм молод, наполнен рвачеством первоначального накопления и удержания капитала. Инновации превращаются в игру, а инновационные центры показывают более чем скромные результаты.

Цифровая экономика – это новая индустриализация, глобальная трансформация промышленности, систем управления. Выполнять программу такой трансформации можно только централизованно. А промышленность приватизирована, разделена частными интересами владельцев, которые могут и не согласиться на глобальную трансформацию.

Стандартизация vs частная собственность

В просоветском сознании возникает идея стандартов цифровой экономики, стандартов «безопасного города», «электронного города», «умного» производства и пр. В прошлом году стандарт «умного» города выпустила рабочая группа при Минстрое, сейчас деятельность по «стандартописанию» передана Российской венчурной компании. Но результатов деятельности нет и, скорее всего, не появится. Причина – противоречия в самих принципах экономики.

Так, Технический комитет 194 «Кибер-физические системы» при РВК в конце января текущего года предложил на общественное обсуждение стандарты «умного» производства как часть стандартов цифровой экономики. Возьмем для примера стандарт на цифровые двойники для «умного» производства. В этом документе объемом более 110 страниц изложено все: понятия, архитектура, взаимодействие с системами «умного» производства и т.д. Обилие англоязычных аббревиатур показывает, что стандарт заимствованный, переписан из каких-то зарубежных документов, но без ссылки на них. Однако в результате оказывается, что речь идет только о конвейерном машиностроительном производстве. Есть ли оно в России помимо оборонной промышленности? Да, как минимум на КАМАЗе, ВАЗе и ГАЗе. Но такие предприятия по пальцам можно пересчитать. И нужен ли этим предприятиям стандарт от экспертов ТК 194 – вопрос открытый.

«Отлить в бронзе» стандарт автоматизации производства можно только тогда, когда есть опыт такой автоматизации, причем накопленный национальными школами и отечественными разработчиками и для отечественного производства. У нас же автоматизацией производства последние 20–30 лет занимались сугубо зарубежные компании – Siemens, ABB, SAP, Oracle, IBM и пр. И продолжают это делать сейчас. Там, на «развитом Западе», эти компании входят в состав рабочих групп, легализуя в рамках стандартов свои лучшие практики. Никто с этим не спорит, стандарт не противоречит инженерной практике, входит в жизнь логично и бесконфликтно. А мы берем эти документы, с умеренным успехом переводим их на русский язык и считаем, что по таким стандартам будет построена цифровая экономика.

Да и собственники самого производства только частично российские, в советах директоров крупнейших предприятий немало иностранцев. Так для кого же стандарт? Для них? Но иностранцы не обязаны следовать мнению умных российских экспертов, имеющих свой взгляд на автоматизацию производства на основе переведенных документов и своего опыта внедрения импортных технологий. И владельцы производства не обязаны следовать мнению авторов стандарта – предприятие находится в частной собственности, политику его автоматизации владелец и определяет. Он обеспечивает рентабельность своего предприятия, сам его организует и сам отвечает за его банкротство, если что-то сделал не так. В самом стандарте нельзя выдвигать какие-либо требования, потому что требовать перестроить производство от субъектов хозяйственной деятельности регулятор не может, это ограничивает конкурентную среду и мешает работе «невидимой руки рынка». Регулятор определяет правила взаимодействия участников рынка, но не вмешивается во внутреннюю кухню их работы, если там не нарушаются нормы закона.

Вот и получается: индустриализацию нужно делать масштабно, по-государственному, а священное чувство частной собственности вмешиваться не позволяет. Остается только писать никому не нужные стандарты, рекомендовать, переписывать зарубежные документы. А развитие пойдет так, как завещал Карл Маркс, – хаотично, без оглядки на стандарты, но с очень пристальным вниманием к бюджетам и прибылям от деятельности. Значит, вся программа цифровой экономики – не более чем государственная вывеска над процессами, которые по своему разумению, но желательно на средства из госбюджета, будут осуществлять участники рынка. С максимальной эффективностью (т.е. прибылью), расчетной монетизацией и по возможности с минимальными затратами на научно-технический прогресс. Занавес. ИКС

Цодостроительная география

Где строить дата-центр? При выборе региона для строительства надо учитывать особенности географии – риски стихийных бедствий, политической нестабильности, доступность ресурсов. Но еще важнее – бизнес-климат и привлекательность для клиентов.

Николай Носов

Когда Ной спросил Бога, где взять животных для Ковчега, тот ответил: «Построй его, и они придут». Эта стратегия оказалась успешной при спасении животного мира от Всемирного потопа, но далеко не всегда работает при развертывании дата-центра. Наличие удобной площадки для строительства и поддержка местной администрации облегчают возведение ЦОДа, но не гарантируют последующего появления клиентов. Так что есть вероятность остаться с замороженными в построенном объекте и не приносящими дохода инвестициями и даже с убытками в виде операционных расходов.

Стихийные бедствия

Согласно исследованию Data Center Risk Index, проведенному компанией Cushman & Wakefield, наибольший вес (15,38%) среди критериев выбора места для строительства ЦОДа имеют риски природных катаклизмов (см. таблицу). Скажем, землетрясения, которые постоянно происходят на планете, могут внести серьезные коррективы в ваши планы. Так, прошлогоднее землетрясение на Филиппинах привело к разрушению зданий, выходу из строя систем обеспечения, коммуникаций и дорог. Даже не очень сильные подземные толчки могут опрокинуть серверные шкафы в дата-центре, разорвать подземные коммуникации или вызвать перебои в электроснабжении.

Помимо высоких рисков разрушения ЦОДа расположение в сейсмоопасной зоне увеличивает капитальные затраты на его строительство, поскольку требует применения дорогостоящих сейсмоустойчивых технических решений. При размещении в прибрежной зоне в Юго-Восточной Азии стоит обратить внимание на угрозу цунами, для российских же реалий более актуальна угроза подтопления в результате наводнений и весенних паводков, особенно когда дата-центр находится на берегу реки или водоема. Угрозу ЦОДам несут и другие природные катаклизмы – сели, ураганы, смерчи.

Политика, энергетика и связь

На втором месте рейтинга – политические риски (12,82%). Действительно, обидно будет построить Ковчег, на котором уплывет кто-то другой. А в политически нестабильных регионах владельцы собственности могут поменяться быстро, как это произошло, например, с первым и единственным украинским дата-центром,

Критерии выбора страны для размещения ЦОДа ▼

Критерий	Вес, %
Стоимость 1 кВт·ч электроэнергии	8,97
Наличие высокоскоростных каналов интернет-доступа	11,54
Легкость ведения бизнеса (согласно рейтингу World Bank)	11,54
Ставки налогов для юридических лиц	6,41
Политическая стабильность (согласно индексу стабильности European University Institute)	12,82
Устойчивость функционирования (доступность электроэнергии от альтернативных источников)	8,97
Вероятность природных катастроф	15,38
Безопасность энергоснабжения	12,18
ВВП на душу населения	5,77
Доступность водных ресурсов	6,41

Источник: Data Center Risk Index компании Cushman & Wakefield

МНЕНИЕ ЭКСПЕРТА

Татьяна Толмачева, партнер, iKS-Consulting

Административный ресурс – важный фактор

При выборе места для строительства дата-центра не стоит забывать о возможностях административной поддержки со стороны региональных властей. Регион может создавать благоприятные условия для строительства ЦОДа – на льготных условиях выделять землю, быстро выдавать разрешения и согласования. По такому пути идут власти Москвы при строительстве телекоммуникационных вышек. Другой вариант – финансовые преференции. Причем иногда, например в ХМАО, возможны даже инвестиции в рамках государственно-частного партнерства. Чаще регион дает льготы в виде сокращения местных налогов, например, на землю или имущество. Сотрудничество по линии ГЧП улучшает показатели возврата инвестиций и минимизирует риски.

Строить или нет? Комплексный рейтинг покажет

Станислав Мирин, ведущий консультант, iKS-Consulting

Доля Москвы и Санкт-Петербурга в бизнесе коммерческих дата-центров сегодня составляет 84%. Однако многие столичные дата-центры устремляют свой взгляд в регионы. Кроме того, мы видим инициативу региональных инвесторов строительства ЦОДов за пределами Москвы и Петербурга. В связи с этим часто возникает вопрос: региональный рынок отстает из-за того, что там нет спроса, или потому, что отсутствует адекватное предложение со стороны коммерческих дата-центров? Ответить на этот вопрос может исследование конкретного региона, в рамках которого перспективы строительства ЦОДа оцениваются по целому ряду макропоказателей, в том числе:

- по активности и динамике экономического развития;
- наличию в структуре экономики региона крупных предприятий из отраслей – потенциальных потребителей услуг ЦОДов;
- наличию в регионе технопарков и других концентрированных проявлений ИТ-активности (выставок, конференций).

Необходимо также исследовать спрос, опросив представителей потенциальных потребителей, и промоделировать его динамику, исходя из возможностей того или иного региона.

Вместе с тем перспективность строительства ЦОДа нужно рассматривать и с точки зрения затрат на его эксплуатацию:

- стоимости электроэнергии (самый важный ресурс для ЦОДа);
- стоимости и доступности специалистов для работы в дата-центре;
- наличия широких каналов связи, их надежности и представленности операторов связи в регионе.

Таким образом, для того чтобы оценить целесообразность выхода в регион с инициативой строительства ЦОДа, необходимо составить комплексный рейтинг.

имеющим сертификат Uptime Institute Tier III. ЦОД «Парковый» в Киеве ввели в эксплуатацию как раз перед Майданом.

ЦОД – крупнейший потребитель электроэнергии. Не удивительно, что на третьем месте в рейтинге идет энергетическая безопасность (12,18%), совсем немного уступающая политической стабильности, а стоимость электроэнергии – на шестом месте (8,97%).

Важны наличие скоростных каналов доступа в интернет и простота ведения бизнеса (по 11,54%). Последнее в российских реалиях часто заключается в возможности задействовать административный ресурс, что напрямую зависит от местных властей.

Новые угрозы

Новый и еще не изученный фактор, влияющий на работу дата-центра, – пандемия. Весенний опыт карантина и самоизоляции показал, что работа дата-центров в регионах с невысокой плотностью населения и, как следствие, с низким уровнем распространения инфекции практически не пострадала – в отличие от ЦОДов, расположенных в Москве и функционирующих в условиях карантинных мер и пропускного режима. Столичным дата-центрам пришлось перейти на новый режим работы с отменой постоянных пропусков, ограничением доступа на территорию контрагентов и клиентов, фактически заморозить деятельность, не связанную с непосредственным обеспечением работоспособности, выполнением жизненно важных для функционирования ЦОДа работ.

Не ясно, когда закончится пандемия, будут ли новые волны вспышек заболевания, где и какой строгости введут карантин, но уже видно, что новый фактор оказывает влияние на работу ЦОДов. Это стоит учитывать, имея в виду вероятность еще более опасных эпидемий, которые могут быстро распространяться по сегодняшнему глобализованному миру.

Строительство ЦОДов в российских регионах

Тактика Ноя «построим – сами придут» иногда работает. Так, у ЦОДа «Авантаж» в подмосковном Лыткарино изначально была хорошая площадка для строительства, подведенные электрические мощности, каналы связи и поддержка местной администрации. Нельзя сказать, что после окончания строительства клиенты бросились раскупать места, но грамотная информационная кампания позволила продать дата-центр МТС, так что проект успешен.

ЦОДы – это современно, модно, это новые рабочие места и улучшение отчетных показателей по выполнению программы «Цифровая экономика

РФ». Региональные власти, как правило, поддерживают инициативы их строительства, более того, каждый регион хочет иметь свой дата-центр. Но чтобы ЦОД не простаивал, «съедая» деньги инвесторов и налогоплательщиков, к выбору места строительства надо отнестись максимально ответственно.

Причем по сравнению с условиями ведения бизнеса все географические предпочтения отходят на второй план. В первую очередь нужно определить бизнес-модель работы дата-центра. Понять, на каких клиентов он рассчитан, какие задачи будет решать, каковы конкурентные преимущества строительства в конкретном регионе, окупит ли строительство инвестиции и насколько быстро.

Важный довод в пользу выбора места строительства – наличие «якорного» клиента, крупной организации с гарантированным спросом на мощности дата-центра. Например, половину емкости ЦОДа, построенного в 2019 г. «Ростелекомом» в Екатеринбурге, заняла компания «Газпром нефть». Хороший якорный клиент – большое промышленное предприятие региона. Хотя тут все не так просто – в перспективе предприятию может стать экономически выгоднее использовать свои ЦОДы, привлекая коммерческие только при пиковых нагрузках. Долгосрочный спрос обеспечат органы государственной власти.

Надо изучать потребности клиентов в каждом конкретном случае. Например, коммерческие ЦОДы могут быть востребованы в качестве площадки для восстановления после аварии и для резервного копирования критичных для бизнеса систем.

Клиенты из других регионов вряд ли захотят использовать «чужой» коммерческий ЦОД по модели colocation – придется перевозить на большое расстояние свое оборудование, а затем ездить его навещать, а это время и дополнительные расходы. Хотя здесь бывают исключения.

По чисто физическим причинам, связанным с задержкой сигнала, не удастся предложить клиентам из других регионов услуги «горячего» восстановления после аварии. Критичны к задержкам в сети облачные игры и многие производственные процессы. Зато можно оказывать услуги архивного хранения данных, «холодного» резервного копирования. Главное – иметь каналы связи с высокой пропускной способностью.

В целом при выборе места для строительства ЦОДа лучше не полагаться на авось и не руководствоваться только удобством строительства и эксплуатации, а тщательно изучить все риски и потенциальный спрос, в том числе с помощью специализирующихся на таких исследованиях консалтинговых организаций, и лишь потом начинать работу. И тогда «звери» придут. ИКС

Аварийное восстановление и облака

Николай Носов

Современный бизнес – непрерывная обработка цифровых данных, потеря которых приводит к авариям, остановке, экономическому ущербу, а в худшем случае – к гибели людей. Поэтому так важны планы, регламенты и инструменты аварийного восстановления данных и ИТ-инфраструктуры.

Остановка – и тебя безнадежно обогнали конкуренты, в тебе начали сомневаться заказчики и партнеры-контрагенты. Нельзя прервать работу доменной печи или сети связи. Если у банка три дня не проходят платежи – ЦБ отбирает лицензию.

Стелим соломку

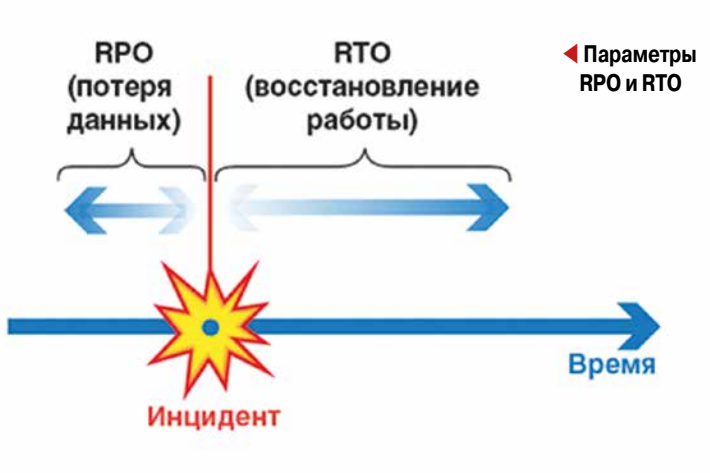
Пожар, землетрясение, атака хакеров, техническая неисправность оборудования – от неприятностей не застрахован никто. Более того, аварией может стать не только пожар или наводнение, но и менее значительное происшествие, например, когда провалился фальшпол и одна стойка упала.

«Знал бы, где упасть, соломку бы подстелил», – гласит известная поговорка. Ответственно относящиеся к работе компании думают, где могут «упасть», и «подстилают соломку» – уделяют внимание непрерывности бизнеса, способности организации даже после разрушительного инцидента продолжать поставлять продукцию или оказывать услуги на приемлемом уровне. Главное – знать, что делать в той или иной ситуации, иметь план аварийного восстановления, включающий пошаговый сценарий действий персонала: кому и по каким телефонам звонить, какое оборудование подключать, какие программы запускать. Первый шаг – оценить аварийную ситуацию, понять, что случилось, по какому сценарию произошла авария. Возможны частичная или полная потеря оперативных данных, выход из строя вычислительного оборудования, сети передачи данных, ЦОДа, перебои энергоснабжения или проблемы с персоналом.

Заранее уполномоченные сотрудники на основании информации дежурных смен пытаются идентифицировать аварийный сценарий, принимают решение об активации частных планов аварийного восстановления. Решение доводится до руководителей подразделений и групп, отвечающих за реализацию плана, которые, в свою очередь, имеют четкие пошаговые документированные и утвержденные инструкции о том, кто что делает и кто за что отвечает.

В утвержденных документах, как правило, содержатся параметры RPO (Recovery Point Objective), т.е. максимальный период времени, потерю данных за который можно считать допустимой, и RTO (Recovery Time Objective), время восстановления работы (см. рисунок).

Допустимые значения RTO и RPO устанавливаются в процессе планирования непрерывности бизнеса с учетом целевого времени восстановления конкретных бизнес-процессов (и соответственно поддерживающих их ИТ-сервисов). В зависимости от заданных RPO и RTO выбираются решения для аварийного восстановления (Disaster Recovery, DR) данных, вычислительной и сетевой инфраструктуры, которые включают в себя политики, инструменты и процедуры восстановления или поддержки жизненно важной технологической инфраструктуры/системы после стихийного или антропогенного бедствия.



Параметры RPO и RTO

Подальше положишь – поближе возьмешь

Самое очевидное решение на случай аварии, – дублирование. Уже довольно популярна схема с двумя серверами, объединенными в кластер. Вышел из строя один сервер – нагрузка автоматически переносится на другой, работающий в режиме «горячего» резерва с синхронным отслеживанием изменений на первом. Возможны варианты, когда часть нагрузки постоянно работает на одном сервере кластера, часть – на другом и соответственно для разных задач разные серверы выступают в качестве основного и резервного.

Еще надежней вариант с двумя СХД, особенно с синхронной репликацией данных, до минимума снижающей RPO. Если каждый сервер кластера связан с каждой СХД, работа остановится лишь в случае выхода из строя дублирующих устройств.

Это хорошо, но недостаточно. Ситуация с одновременным отказом дублирующих устройств в одной серверной не такая уж редкость. В банке, где я долгое время работал, серверная находилась на верхнем этаже под крышей. В сильную жару крыша нагревалась, кондиционеры не справлялись с нагрузкой и выходили из строя. Когда температура в серверной поднималась до критической отметки, оба сервера кластера выключались. Приходилось в авральном режиме заниматься откачиванием горячего воздуха, дополнительно устанавливая напольные кондиционеры. Работа банка на это

время останавливалась, ведь на кластере размещалась АБС.

Пожар в серверной, перебои с электропитанием, обрыв линии связи – в этих случаях дублирование оборудования в одной серверной не поможет. Надежнее разместить дубли критически важных для бизнеса систем на другой площадке, например, создав растянутый кластер из серверов, расположенных в разных ЦОДах. Скажем, чтобы в Москве гарантированно иметь независимое электропитание, можно выбрать дата-центры на разных берегах Москвы-реки.

Для восстановления информационной системы после аварии можно задействовать как свои, так и арендованные дата-центры – с арендой площадей ЦОДа по модели colocation для собственного оборудования, арендой физического оборудования дата-центра либо вообще с использованием облачных услуг провайдера.

«Холодно», «теплее», «горячо»

Разнесение площадок по регионам поможет решить проблему выхода из строя ЦОДа из-за стихийных бедствий: землетрясений, наводнений, ураганов, цунами. Разнесение по странам призвано уберечь от последствий политической нестабильности. Однако из-за ограниченной скорости прохождения сигнала и пропускной способности каналов связи придется отказаться от синхронной репликации. Увеличивается RPO, резервное копирование становится «теплым» или даже «холодным».

Выбор решения зависит от конкретных задач и величины потерь вследствие простоя информационных систем. Иметь в «горячем» резерве ЦОД с синхронной репликацией всех данных хорошо, но очень дорого и, как правило, экономически не оправдано. Чаще на случай аварии достаточно иметь резервную копию (бэкап) и площадку для разворачивания резервного ЦОДа и восстановления системы из бэкапа.

Традиционные подходы к Disaster Recovery предполагают наличие у компании резервного ЦОДа и одного из трех вариантов резервирования: «холодного», «теплого» или «горячего». Границы между этими терминами эксперты понимают по-разному, в общем случае исходя из времени, требуемого на восстановление.

«Холодное» резервирование предполагает наличие резервной площадки (серверного помещения или ЦОДа), оснащенной необходимыми инженерными установками, где можно оперативно развернуть ИТ-оборудование для запуска резервной системы. Часть такого оборудования может храниться на складе, часть – закупаться или арендоваться по мере необходимости. Как правило, каналы связи в «холодный» ЦОД заводятся заранее, но активация телекоммуникационных сервисов производится только после принятия решения о его запуске. Понятно, что время запуска такого ЦОДа (другими словами, значение RTO процедуры Disaster Recovery) достаточно велико (может превышать неделю).

В случае «теплого» резервирования альтернативная площадка оснащается всем необходимым ИТ-оборудованием; каналы подключения к интернету и корпоративной WAN-сети находятся в активном состоянии. На «теплой» площадке имеется резервная копия данных: актуальность данных поддерживается путем физической перевозки резервных копий на лентах или организацией бэкапа по сети передачи данных из основного дата-центра. Типовое значение RTO для процедуры Disaster Recovery при «теплом» резервировании превышает день.

При «горячем» резервировании альтернативная площадка представляет собой полное «зеркало» основного ЦОДа. Если ЦОДы работают по схеме active – active, данные в них обновляются синхронно, а в менее дорогостоящей схеме active – passive выполняется асинхронная репликация. Репликации осуществляются на уровне системы хранения данных (функция синхронной репликации поддерживается большинством СХД даже среднего уровня), на уровне сервера или приложения, например СУБД (включая продукты Oracle, Microsoft SQL Server, MySQL, PostgreSQL). В работе могут быть задействованы оба ЦОДа с балансировкой и распределением нагрузки между ними.

При синхронной репликации приложения в реальном времени записывают данные сразу на обе площадки географически растянутого кластера. Чтобы приложения не «тормозили», время отклика должно составлять порядка 5 мс. За это время второй ЦОД должен получить информацию и подтвердить ее получение. Время прохождения сигнала зависит от длины проложенного оптического кабеля. По оценке руководителя направления СХД «Инфосистемы Джет» Романа Харыбина, такое время отклика воз-

Александр Тугов, директор по развитию услуг, Selectel

Территориальная разнесенность дата-центров – важный критерий для сценариев с низкими значениями RPO/RTO, а также с рисками природных бедствий и аварий на объектах инфраструктуры. В российских условиях нормой считается расстояние между объектами от 30 км, для стран с большей вероятностью природных катаклизмов (например, США) – обычно от 140 км.

можно, если ЦОДы удалены друг от друга не более чем на 30–50 км. Обычно расстояние между дата-центрами при «горячем» резервировании с синхронной репликацией стараются ограничить 25–30 км.

При асинхронной репликации расстояния не так критичны, зато важна полоса пропускания, выдерживающая поток данных между площадками. Определить полосу пропускания нужно еще до заключения договора аренды или строительства нового ЦОДа.

Помимо данных, используемых приложениями, между площадками должны постоянно синхронизироваться настройки ИТ-оборудования, версии ОС, обновления системы безопасности и пр. При наличии «горячего» резервного ЦОДа значение RTO может ограничиваться минутами. Но из трех перечисленных вариантов резервирования этот вариант самый дорогостоящий в реализации и обслуживании.

В каждом из трех вариантов требуется иметь в резерве удаленную площадку с определенным набором оборудования, что само по себе стоит дорого, особенно если компания решает сама строить и обслуживать такую площадку (а не использовать услуги colocation). В случаях «теплого» и «горячего» резервирования предполагается наличие дорогостоящего ИТ-оборудования (стоимость которого может на порядок превышать стоимость инженерных систем ЦОДа), которое будет простаивать в ожидании катастрофы. Неудивительно, что до недавнего времени системы Disaster Recovery могли себе позволить только очень богатые организации, как правило, из финансового сектора. С появлением и распространением технологий виртуализации, а особенно с появлением услуг облачного резервного копирования и аварийного восстановления схемы Disaster Recovery становятся доступными все более широкому кругу заказчиков.

Очень холодно, прямо ледник

Традиционный способ сохранения данных на случай аварийной ситуации – создание резервных копий. Без резервного копирования (бэкапа) невозможно представить работу бизнеса – даже в самом маленьком предприятии важная информация копируется как минимум на флешку.

По сравнению со схемами с резервным ЦОДом обычный бэкап – дешевый, но менее катастрофоустойчивый вариант восстановления бизнес-процессов. Вычислительная и сетевая инфраструктуры не дублируются – данные копируются на носители в том же или стороннем дата-центре и вновь переносятся на оборудование основного дата-центра после ликвидации последствий аварии и возобновления работы его инфраструктуры.

Резервное копирование развивается вслед за лавинообразным ростом объема хранимых данных. Данные становятся все более ценным и невосполнимым активом: использование первичных документов понемногу отмирает, остаются только электронные копии, которые нужно защищать от потери. В России, в отличие от остального мира, предпочтение отдается собственным ЦОДам. Тенденция использовать две или три площадки сохранится. Сейчас, когда многие компании пересматривают ИТ-бюджеты, выбор будет смещаться в сторону аутсорсинговых услуг. В краткосрочной перспективе они обходятся дешевле.

Роман Харыбин, руководитель направления СХД, «Инфосистемы Джет»

Копировать можно наборы файлов, базы данных, операционную систему (файлы ОС), диски или дисковые тома целиком (посекторно или поблочно). Для хранения используются диски, ленты или виртуализированные носители – виртуальные диски виртуальных машин (блочные хранилища), файловые и объектные хранилища.

Резервное копирование отдельных систем позволяет восстановить работу после ошибочных действий персонала или атак злоумышленников, например, с помощью вирусов-шифровальщиков. Часто резервные копии используются как тестовые базы для разработчиков. Бэкапы стоит периодически проверять на возможность восстановления, чтобы не столкнуться с ошибкой в критической ситуации.

Часть старых резервных копий отправляют в архив для длительного хранения. При необходимости система может быть восстановлена из архива, но поскольку вероятность такого события мала и снижается с возрастом резервной копии, архивы записывают на дешевые медленные носители. С этой точки зрения архивирование можно рассматривать как «очень холодное» резервирование. Не зря в AWS хранилище такой информации называют Glacier (ледник). В архив отправляют и отдельную важную информацию, например отчетную, которую нужно хранить определенное время в соответствии с политиками компании или требованиями законодательства. Это информация имеет самостоятельную ценность для использования в будущем и не предназначена для восстановления.

DRaaS – помощь из облака

Облака обеспечивают гибкость и скорость развертывания услуги, что справедливо и для сервисов резервного копирования и аварийного восстановления. Однако обосновать перед руководством компании затраты на не работающую постоянно инфраструктуру нелегко.

Резервная площадка в облаках

Появление услуг облачного резервного копирования и аварийного восстановления сделало схемы Disaster Recovery более доступными широкому кругу заказчиков. При этом могут быть реализованы следующие сценарии:

- «горячее» аварийное восстановление (Disaster Recovery as a Service, DRaaS) – запуск параллельной «боевой» инфраструктуры в облаке с возможностью эластичного масштабирования;
- «холодное» («теплое») DRaaS – создание актуальных копий инфраструктуры в облаке. При аварии время нужно только на ее развертывание;
- резервное хранение (BaaS) – создание копии данных в облаке на носителе (дисковом хранилище, ленте...), предназначенной для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения;
- долговременное хранение архивных данных (электронных документов в неизменном виде) в облаке или на физических носителях.

Модель DRaaS предполагает, что сервис-провайдер берет на себя работу по восстановлению функционирования ИТ-приложений и сервисов заказчика в случае аварии основного ЦОДа.

При выборе сервиса DRaaS компании не надо заботиться об организации и оборудовании резервной ИТ-площадки, тратить немалые средства на ее развертывание и обслуживание. В качестве такой площадки будет задействован коммерческий ЦОД провайдера сервиса. В случае аварии на основном объекте и переноса нагрузки на резервную площадку она начнет потреблять ресурсы, и заказчику придется платить больше.

Менее дорогой вариант Disaster Recovery – резервное копирование данных в облако (BaaS). Данные будут использованы в случае аварии в основном ЦОДе. Частный случай BaaS – резервное копирование в облаке на ленту (Tape as a Servise, TaaS) и соответственно восстановление с нее.

Хорошо иметь резервную площадку в облаке

Преимущества услуг облачного резервного копирования и аварийного восстановления во многом определяются общими достоинствами облачной модели.

Экономия средств. Не надо строить ЦОД, закупать оборудование и поддерживать его работу. Отдельно стоит отметить edge-ЦОДы предприятий, функционирующие в неблагоприятных условиях. Наличие страхующего виртуального двойника в облаке позволяет использовать менее дорогостоящие решения для их защиты.

Простота реализации (комплексное решение «из одних рук»). Самостоятельное развертывание решений Disaster Recovery требует планирования, проектирования, внедрения и обслуживания разнообразных систем, что подразумевает наличие собственной экспертизы в компании или привлечение внешних интеграторов. В случае DRaaS эта работа выполняется сервис-провайдером.

Простота масштабирования. Всю работу по добавлению или сокращению необходимых ресурсов – серверов, СХД, средств обеспечения

коннективности площадок – осуществляет провайдер. Заказчик получает ровно те ресурсы, которые необходимы для выполнения его задач.

Гибкость. При использовании DRaaS компания не привязана к конкретной технологии или проприетарным системам, что позволяет применять наиболее подходящие решения.

Простота тестирования. В традиционных схемах Disaster Recovery тестирование – процесс сложный, трудозатратный и рискованный: можно потерять рабочую систему. Применяемые в DRaaS решения автоматического управления виртуальными машинами, резервированием и репликацией данных обеспечивают простое безопасное тестирование. Более того, облачные провайдеры могут предоставить изолированную тестовую зону для отработки сценариев аварийного переключения.

Облачные услуги реализуют резервное копирование и аварийное восстановление с помощью наиболее экономически выгодных решений, что дает конкурентные преимущества компаниям, в том числе небольшим, которым ранее дорогие технологии были не по карману. Примеры специализированных решений DRaaS: Commvault Simpana, Dell EMC Avamar, Veritas Resiliency Platform и Veritas InfoScale, VMware vCloud Availability. На российском рынке, по данным iKS-Consulting, наиболее популярен продукт Veeam Backup & Replication, предназначенный для резервного копирования виртуальных машин VMware и Hyper-V.

Какие сложности скрываются в облаке

При пользовании услугами DRaaS важен вопрос доверия к поставщику облачных услуг, получающему доступ к резервируемым данным. Стоит изучить партнерские статусы провайдеров, объем предоставляемых ими услуг. «При выборе аутсорсинговой компании следует оценить ее способность не только оказывать услуги на требуемом уровне, но и обеспечить защиту резервируемых данных», – подчеркивает руководитель отдела ЦОД компании «ЛАНИТ-Интеграция» Юрий Барабанщиков. Если в резервных копиях, которые передаются на внешнюю площадку, содержатся персональные данные, то информационные системы провайдера должны быть аттестованы в соответствии с требованиями 152-ФЗ.

Важна и гарантированная пропускная способность линий связи между основной и резервными площадками, иначе есть риск не успеть сохранить или восстановить данные. «Необходимо также подумать о совместимости форматов хранения и используемого ПО резервного копирования на собственной и удаленной площадках. Чтобы тратить время только на транспорт данных, а не на конвертацию или переподготовку извлеченных “холодных” данных. Как правило, в собственных системах эти вопросы решаются проще», – предупреждает Роман Харыбин, руководитель направления СХД компании «Инфосистемы Джет».

Другой момент, на который стоит обратить внимание, – тестирование резервных копий, расположенных на площадке провайдера. Компания должна быть уверена, что в аварийной ситуации все пройдет по плану. Однако бывали случаи, когда сервис-провайдер не давал возможности обратного скачивания данных при аварийном восстановлении.

Часто проблемы возникают при развертывании на стороне облачного провайдера сетевой инфраструктуры заказчика. Даже если провайдер предоставляет услугу SDN, то за исключением простейших случаев необходимо заранее провести работы по адаптации инфраструктуры, на которую перейдет заказчик в случае аварии и переноса вычислительных мощностей в облако. И нужно не забыть при этом о воспроизведении в облаке политик безопасности, принятых в компании.

Согласование DRaaS со службой информационной безопасности предприятия – отдельная и не всегда решаемая задача. Например, в «Почте России» для этих целей разрешено задействовать только физически выделенное у провайдера облако – служба ИБ запрещает делить вычислительные ресурсы с посторонними организациями. Другой допустимый вариант – использование модели colocation. По такой модели DR и резервное копирование организуют Райффайзенбанк и группа компаний «Медси».

Настороженно к использованию коммерческих ЦОДов относятся государственные организации. Так, в фонде ОМС считают, что к облачному хранению архивов можно будет обратиться после появления ГЕОП.

Как правило, представители службы ИБ заказчика выезжают на место и оценивают защищенность данных в коммерческом дата-центре, его ресурсы, технологические и бизнес-процессы. Анализируются все возможные риски, в том числе потенциальные конфликты собственников.

Компания несет полную ответственность за свои данные. Конечно, облачный провайдер дорожит своей репутацией и сделает все возможное, чтобы ее не потерять, но юридически его ответственность невелика и ограничена SLA. Никто кроме компании не разработает политики хранения и восстановления данных. Сервис-провайдер может проконсультировать по процедурам аварийного восстановления и обеспе-

чения непрерывности бизнеса, но даже если их предложит высококвалицированный специалист, выполнять их будет клиент.

Дополнительная проблема – обоснование затрат на услугу DRaaS. Руководству компании не всегда очевидно, зачем платить за ресурсы, которые постоянно выключены. Любые затраты на мероприятия по обеспечению непрерывности бизнеса и катастрофоустойчивости нужно обосновывать в контексте соответствующих планов предприятия. «Формирование таких планов (и даже осознание их необходимости) требует зрелости предприятия, поддержки со стороны первых лиц компании, а также комплексного анализа влияния аварийных ситуаций на бизнес-процессы, доходы и затраты предприятия. К сожалению, далеко не все предприятия, даже крупные, такой анализ провели», – указывает Владимир Ткачев, технический директор VMware в России и СНГ.

Тем не менее низкий порог вхождения в DRaaS позволяет стартовать с малого – резервировать в облаке наиболее критичные компоненты ИТ-инфраструктуры предприятия, а в некоторых сценариях использовать облако провайдера как место для временного размещения ресурсов на время обновления собственной инфраструктуры.

Аварийное восстановление завтра

Оркестрация и оптимизация процессов восстановления, снижение требований к каналам связи, работа в гибридных и мультиоблачных средах – вот основные направления развития решений аварийного восстановления.

Больше автоматизации

В далекие годы перестройки после окончания МИФИ я принимал участие в разработке высокопроизводительного специализированного компьютера. Вычислительных мощностей не хватало, поэтому работали круглосуточно. Под утро, по окончании ночной смены, вручную сбрасывал наработанное отделом за ночь на резервный диск. Набирал в командной строке команду copy с указанием источника и приемника, но однажды, заработавшись, их перепутал и скопировал данные из резервной базы на основную, уничтожив работу отдела за ночь.

Ошибки персонала неизбежны, а цена их может быть высока. Работу по резервному копированию и восстановлению следует максимально автоматизировать. Как минимум – написать скрипты с командами копирования. Задача максимум – сделать выполнение планов аварийного восстановления автоматическим. К сожалению, в полном объеме это пока невозможно, поскольку в планы входят и организационные меры. Но повышение уровня автоматизации – одно из направлений развития DR.

В случае DRaaS задача автоматизации усложняется закрытостью инфраструктуры облачного провайдера. Более того, заказчик часто имеет не только виртуальную, но и физическую инфраструктуру, так что для сложных решений аварийного восстановления потребуются персонализированные проекты. С ростом популярности DRaaS и усилением конкуренции между поставщиками услуг стоит ожидать расширения номенклатуры предлагаемых типовых инфраструктурных решений, большей гибкости провайдеров в вопросах предоставления инфраструктуры.

Восстанавливать только необходимое

Причина популярности схемы «горячего» резервирования ЦОДов – простота принятия решения: не работает один – стартует другой. Причем все происходит автоматически и без потерь. Так можно держать включенным второй телевизор, чтобы в случае поломки основного не пропустить забитый гол. Но в случае ЦОДа подобный подход обойдется в слишком большую сумму.

Дешевле, но гораздо сложнее, – выявить неработающие узлы и восстановить только пострадавшую инфраструктуру. Это может оказаться нетривиальной задачей, требующей оркестрации – запуска виртуальных машин в определенной последовательности в зависимости от состояния других виртуальных машин. Напри-

мер, не включать сервер приложений, пока не будет работоспособен сервер с Active Directory. Или ранжировать неработающие приложения по степени важности для бизнеса и запускать в первую очередь наиболее критичные.

Такие решения аварийного восстановления не коробочные, зависят от технологических процессов конкретной организации. Сначала надо описать процессы, понять логику – в какой последовательности должны переезжать системы, а потом пытаться автоматизировать восстановление. Это сложно – заказчик не всегда понимает внутренние бизнес-процессы. Но решения для оркестрации уже предлагаются, например, Veeam Availability Orchestrator поможет автоматизировать процессы восстановления между двумя площадками заказчика.

Оптимизация процессов

Развиваются технологии, возрастает скорость вычислений, дешевле обходится хранение, увеличивается скорость резервного копирования и аварийного восстановления. Общие направления совершенствования систем аварийного восстановления – терять при аварии меньше данных, снижать RTO, оптимизировать хранение, уменьшать стоимость работ.

Совершенствуются технологии, использующие дедупликацию – алгоритмы сжатия, исключающие дублирование копий повторяющихся данных. Использование методов дедупликации позволяет оптимизировать дисковое пространство систем хранения данных, разгрузить каналы, передавая только изменение данных.

Сжатые дедуплицированные копии виртуальных машин занимают мало места, но требуют много времени на восстановление. С удешевлением дисков более доступными становятся реплики – полные копии виртуальных машин, которые, как правило, лежат на более быстрых и дорогих дисках продуктивной системы и полностью готовы к старту. Восстановление с помощью реплик занимает минуты.

Новые технологии

Два года назад на международном энергетическом форуме «Российская энергетическая неделя» рассказывалось о проекте резервного копирования технологических данных с помощью блокчейна. В тот момент технологии распределенного реестра находились на пике хайпа, и их пытались применить везде, где только можно. Пилот так и остался пилотом, блокчейн – это медленно, дорого и мало пригодно для резервного копирования технологических данных энергетических компаний. Но сама идея правильная – используемые для аварийного восстановления резервные копии нуждаются в защите, чтобы сохраненные данные никто не смог исказить. А распределенные реестры – лучший способ хранения «общей правды», чувствительной информации, требующей повышенной конфиденциальности.

В блокчейне эффективнее хранить не сами резервные копии, а их хэш, подтверждающий правильность и целостность сохраненных данных. Например, с помощью продукта Acronis True Image 2017 New Generation музыканты и художники подтверждают дату и время создания своих произведений, предоставляя в качестве доказательства сертификат Acronis Notary с указанием этой информации. С помощью функционала Acronis ASign можно подписывать резервные копии документов с автоматической нотаризацией.

> Для защиты данных небольших компаний можно применять дедупликацию на уровне клиента с передачей в ЦОД только уникальных блоков данных. Причем для таких типов данных, как файлы, виртуальные машины и БД Oracle, можно отслеживать и считывать только измененные данные без нагрузки на клиента с последующим синтезом из них полной резервной копии в режиме реального времени на пуле дедупликации в ЦОДе. Для более сложных инфраструктур со значительными объемами данных рекомендуется выполнять резервное копирование на пулы дедупликации локальной автономной системы резервного копирования данных с последующей репликацией только уникальных блоков данных в систему резервного копирования, расположенную в ЦОДе.

Гибридные и облачные среды тоже нуждаются в резервировании

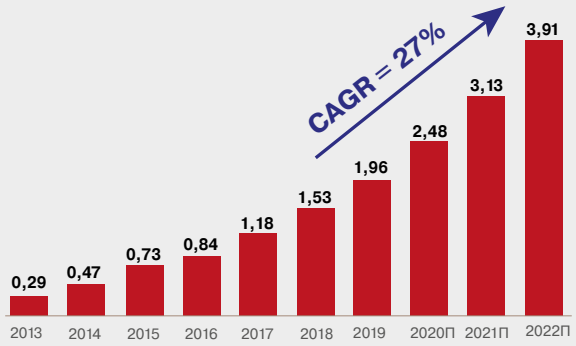
Использование облаков для хранения резервных копий on-premise-систем вошло в повседневную практику бизнеса. Новый этап развития облачных технологий – переход к гибридным облакам. Сложность текущего момента заключается в том, что нужно копировать не только данные и виртуализированную инфраструктуру на площадке заказчика, но и облачную составляющую системы, зачастую расположенную в облаках разных провайдеров и даже на разных облачных платформах.

Александр Тетюхин, технический консультант, Veritas

Рис. 1. Использование облачных услуг хранения и восстановления данных предприятиями разных типов

Источник: iKS-Consulting

Рис. 2. Динамика сегмента Baas/DRaaS (базовый прогноз, млрд руб.)



Источник: iKS-Consulting

Задача свободного переноса виртуализированной инфраструктуры в произвольном направлении еще не решена, но вендоры над этим работают. Шагом на этом пути стал выпуск новой версии продукта Veeam Availability Suite, которая поддерживает резервное копирование в гибридных облаках, включающих AWS, Microsoft Azure и IBM Cloud.

Мультиоблачный подход помогает реализовать правило «3-2-1», которое гласит, что для надежного хранения нужны три копии, физически находящиеся в разных местах, на двух типах носителей, причем одна копия должна храниться вне офиса. Если компания пользуется облачными сервисами, то копии должны храниться на площадке клиента и в двух разных облаках.

Что в тренде?

Рынок облачных услуг ежегодно демонстрирует двузначный рост. Объемы хранимых и обрабатываемых данных также стремительно растут. Оба фактора стимулируют спрос на DRaaS. Кроме того, в условиях экономической рецессии и неопределенности отказ от крупных инвестиций и переход к сервисной модели становятся актуальными для многих предприятий. «По нашим оценкам, глобальный рынок услуг DRaaS будет увеличиваться на 42% в год и к 2022 г. составит около $12 млрд, – отмечает Владимир Ткачев, технический директор VMware в России и СНГ.

Россия движется в этом русле с некоторым временным лагом. Согласно данным опросов iKS-Consulting, сервисы DRaaS – одни из наименее популярных у отечественных потребителей облаков (рис. 1), их используют только 9,2% респондентов.

Чаще других прибегают к услугам DRaaS средние по размеру компании, которые уже осознали необходимость обеспечения непрерывности критических бизнес-процессов, но не имеют средств создать для этого собственную инфраструктуру. Крупные компании могут позволить себе иметь корпоративный резервный ЦОД, но и они в целях экономии все чаще смотрят в облака. И крайне привлекательны с точки зрения обеспечения непрерывности бизнеса облачные услуги для малых предприятий – вопрос в цене таких услуг и зрелости руководства компаний.

По оценкам iKS-Consulting, российский рынок облачного резервирования и аварийного восстановления составляет примерно 9% общего объема рынка IaaS, в 2017–2018 гг. его объем достиг соответственно 1,2 и 1,5 млрд руб. (рис. 2), увеличившись за год соответственно на 40 и 30%.

В условиях цифровизации экономики и повышения требований к непрерывности бизнеса спрос на услуги BaaS/DRaaS будет расти, и до 2023 г. следует ожидать роста в среднем не менее чем на 27%. Дополнительным драйвером станет ситуация на рынке, связанная с непредсказуемым развитием пандемии, которая существенно ограничивает капитальные затраты на новые проекты, – облачные модели позволят решать задачи обеспечения непрерывности бизнеса без существенных капитальных вложений. ИКС

Юрий Барабанщиков, руководитель отдела ЦОД, «ЛАНИТ-Интеграция»

Ограничения на удаленность резервного ЦОДа накладывает параметр RPO – допустимая точка восстановления. Если RPO позволяет, то с помощью современных технологий и продуктов можно оптимизировать использование различных элементов инфраструктуры. Например, дедупликация данных на удаленных площадках и репликация только уникальных блоков между ними могут значительно снизить требования к пропускной способности каналов связи.

NEW

Rittal – The System.

Faster – better – everywhere.

VX IT – самый быстрый IT-шкаф в мире!

- **Выбор индивидуального IT-шкафа**
- **Модульная система компоновки**
- **Быстрая реализация IT-проектов**

Реклама

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

RITTAL

FRIEDHELM LOH GROUP

www.rittal.ru

Rittal VX IT: быстрее, легче, стабильнее

Отвечая запросам отрасли на ускоренный ввод в строй новых ЦОДов, компания Rittal выпустила обновленную линейку оборудования для ИТ-инфраструктуры RiMatrix Next Generation. Ее флагман – шкаф VX IT – отличается простотой конфигурирования и монтажа.

Борис Васильковский, менеджер по продукции IT, Rittal

Шкаф Rittal VX IT пришел на смену хорошо зарекомендовавшему себя у пользователей шкафу TS IT. Буквы VX в названии говорят об используемом пространственном сварном каркасе VX 25, состоящем из горизонтальных и вертикальных профилей. Снаружи на него навешиваются внешние детали шкафа, а внутрь устанавливаются 19-дюймовые профили.

Каркасная рама предыдущего поколения называлась TS8, а шкаф для ИТ-инфраструктуры на ее основе – соответственно TS IT. Максимальная высота шкафов TS IT составляла 47U, а если требовалось больше, приходилось заказывать специзделия. Появившийся в 2018 г. новый каркас VX 25 сначала использовался как основа для промышленных шкафов, впоследствии стал базой для сетевых и серверных напольных шкафов Rittal. В линейке VX IT максимальный каталожный размер шкафа увеличился до 52U.

Увеличенная высота новых ИТ-шкафов Rittal позволит разместить больше оборудования на единицу площади и сэкономить дорогостоящее место в ЦОДе. Оценят эту возможность и проектировщики edge-систем, которые смогут формировать более компактные конфигурации, в пределе состоящие из одного шкафа, но вмещающие в себя и систему бесперебойного питания, и систему пожаротушения (которая у Rittal занимает всего один юнит), и интеллектуальную систему энергораспределения – новые PDU с расширенными интеллектуальными функциями, и целевое оборудование клиента. На основе шкафа VX IT можно создавать ИТ-инфраструктуры с беспрецедентной скоростью, будь то один сетевой шкаф или целый дата-центр.

Нагрузочная способность

Новые шкафы выпускаются в двух исполнениях – для большей и меньшей нагрузки. Шкафы VX IT standard имеют нагрузочную способность 1,5 т, а у моделей VX IT dynamic нагрузочная способность повышена до 1,8 т. Эти шкафы можно установить на роликовые опоры и перемещать по ровной поверхности с 1 т оборудования внутри. Версии отличаются толщиной металла 19-дюймовых профилей и крепежом. У стандартных шкафов толщина 19-дюймовых несущих уголков 2 мм, а у VX IT dynamic – 2,5 мм.

Увеличение толщины металла на весе шкафа сказывается незначительно. Во-первых, каркасы VX IT сварные, а не свинченные, во-вторых, передняя дверь изготовлена из алюминия, за счет этого шкафы Rittal одни из самых легких на рынке – средний вес пустого шкафа с 19-дюймовым интерьером и стенками менее 100 кг. Добавочные 0,5 мм толщины на профилях дают незначительную прибавку на фоне веса устанавливаемого в шкаф оборудования. Поэтому заказчик должен рассчитывать возможности своих перекрытий исходя прежде всего из веса оборудования, а не шкафа.

Новый сварной каркас более устойчив, у него большая сопротивляемость к скручиванию. На внешнем монтажном уровне каркаса можно монтировать несущие элементы снаружи, сняв боковую стенку и не влезая внутрь шкафа.

Все шкафы имеют сертификат, свидетельствующий о том, что изделие предварительно протестировано независимой, сертифицированной в Германии лабораторией Rittal. Шкафы имеют международный сертификат UL 2416, подтверждающий их высокое качество и нагрузочную способность.

Область применения

Шкафы VX IT могут служить в качестве сетевых кроссовых шкафов, этажных распределителей, как шкафы для серверов или как шкафы с высокой степенью защиты от внешних

факторов. На промышленных объектах часто применяются шкафы с сертификатом на степень защиты IP 55 (защита от пыли и кратковременных струй воды) с застекленной передней дверью, глухой крышей, дном и задней дверью.

Шкафы VX IT standard ориентированы в первую очередь на использование в дата-центрах при статической неперемещаемой нагрузке. Их нагрузочная способность в 1,5 т удовлетворяет требованиям большинства заказчиков.

Шкафы VX IT dynamic применяются в проектах с большой нагрузкой, например, в системах высокопроизводительных вычислений, при большом количестве плотно упакованных блейд-серверов, для тяжелых источников бесперебойного питания. Если шкаф типа dynamic размещен в ограниченном пространстве, то его можно установить на роликовые опоры и при необходимости повернуть и получить доступ сбоку или сзади. Такой шкаф можно выдвинуть из линейки шкафов дата-центра, повернуть, что-либо добавить, а потом снова закатить в линейку.

Для edge-решений компания Rittal выпускает системы бесперебойного питания, пожаротушения, контроля управления доступом, управления питанием. Специально под VX IT разработана система внутришкафного охлаждения, для которой 19-дюймовый интерьер асимметрично смещается к боковой стенке, а в освободившееся место устанавливается кондиционер, который будет охлаждать размещенное в шкафу оборудование. Такая система может быть смонтирована в стандартном шкафу.

В линейке RiMatrix Next Generation имеются и антивандальные сейфы, с предустановленной стойкой VX IT внутри. Из других усовершенствований можно отметить ручки с беспроводным контролем доступа, обновление системы мониторинга и расширение функционала блоков интеллектуальных розеток PDU.

Легкость монтажа

Обновленная линейка шкафов облегчает работу монтажникам. Двери теперь монтируются и демонтируются без применения инструментов. Если нужна перенавеска с правой стороны на левую, то дверь легко снимается с петель. После этого демонтируются и перевешиваются на другую сторону шарниры на винтах, дверь переворачивается, снимается и переворачивается ручка. Весь процесс займет несколько минут.

Панели, закрывающие основание шкафа, привинчиваются напрямую к каркасу шкафа, а не устанавливаются, как раньше, на специальные уголки, которые требовалось предварительно монтировать. Появился такой интересный элемент, как двухсекционная, разделенная по вертикали боковая стенка. Каждая секция разблокируется изнутри шкафа и открывается как дверца. Так что и к передней, и задней части шкафа можно получить доступ сбоку, не снимая боковую стенку.

Плоские детали, например боковые стенки и двери, устанавливаются быстро и просто благодаря защелкам и элементам позиционирования. Без помощи инструментов ставятся в шкафы PDU. Раньше их размещали лишь между боковой стенкой и 19-дюймовым профилем, теперь появилась возможность монтажа на вертикальную кабельную трассу – в любом месте шкафа.

Быстрота конфигурирования и поставки

Подобрать конфигурацию шкафа можно как вручную, так и в онлайн-конфигураторе RICS (Rittal Configuration System), где создается 3D-модель, которую клиент может использовать при дальнейшем проектировании. В режиме онлайн конфигурируется любой вариант двери, отдельные 19-дюймовые плоскости с различными кронштейнами для монтажа, различные потолочные панели. Все это стало стандартными изделиями. Например, можно взять каркас необходимого размера и на его основе собрать шкаф в требуемой конфигурации. Также клиент может удаленно обратиться со своими требованиями в отдел технической поддержки и в короткий срок получить готовое решение.

Поставки продукции осуществляются из Германии. У Rittal четыре склада в России – в подмосковном Подольске, Санкт-Петербурге, Екатеринбурге и Новосибирске, где поддерживается постоянное наличие широкой номенклатуры продукции. Такой подход позволяет ускорить и упростить доставку в любую точку России.

В академии Rittal проводят семинары и вебинары, на которых рассказывают о новинках оборудования компании. При необходимости проводятся курсы специализированного обучения партнеров. Все записи семинаров с описанием технических преимуществ продукции размещены на канале компании в YouTube – Rittal Russia.

Дата-центры без дизель-генераторов В начале пути

Почти в каждом ЦОДе мечтают заменить генераторы более современными и экологичными системами. В ближайшие годы мы вряд ли станем свидетелями полного отказа от генераторов, но доля рабочей нагрузки, для которой они резервируют электропитание, будет сокращаться.

Энди Лоуренс, исполнительный директор по исследованиям, Uptime Institute

В 2012 г. Microsoft объявила о планах избавиться от дизель-генераторных установок (ДГУ) в своем парке ЦОДов в Куинси (шт. Вашингтон, США). Шесть лет спустя та же компания для схожей площадки запросила разрешение установить 72 дизель-генератора с планируемым сроком службы не менее десяти лет. Этот пример наглядно показывает, насколько важны ДГУ для средних и крупных ЦОДов. Немногие – очень немногие – могут сегодня хотя бы вообразить себе дата-центр без генератора.

Почти любой оператор и владелец дата-центра хотел бы убрать дизель-генераторы и заменить их более современными и экологически чистыми системами автономного электропитания. Генераторы грязны: они выделяют не только углекислый газ, но и твердые частицы, что означает регуляторные и эксплуатационные ограничения. Генераторы дорого стоят. Они простаивают большую часть времени и создают существенные эксплуатационные накладные расходы: их надо регулярно тестировать, гарантировать выполнение все более жестких нормативных требований, управлять процессами, связанными с обеспечением топлива – доставка, проверка качества, хранение, слив и пр.

Но при всех недостатках дизель-генераторов на сегодняшний день никакая другая технология не сочетает в себе так эффективно низкие эксплуатационные расходы, высокую плотность энергии, надежность, преимущества локального управления и практически неограниченной подачи электричества – пока поставляется топливо.

Неужели все изменится? Не полностью, не сразу и не резко... но да, изменится. Мотивация к отказу от дизель-генераторов все сильнее, особенно у крупнейших операторов (большинство из них уже снизили насколько возможно выбросы углекислого газа, и генераторы остаются главным источником загрязнений). И сочетание новых технологий, таких как топливные элементы, литий-ионные аккумуляторные батареи и современное ПО управления, становится все более эффективным. Хотя полностью и повсеместно от ДГУ, конечно, не откажутся, но мы ожидаем, что уже с нынешнего года их доля будет сокращаться во все большем числе проектов по построению или модернизации ЦОДов.

Можно выделить четыре направления деятельности, касающиеся разработки новых технологий и их внедрения, которые приведут к тому, что в будущем роль дизель-генераторов в ЦОДах будет снижаться – или вообще сойдет на нет.

Топливные элементы и непрерывная генерация на площадке

Возможность замены генераторов топливными элементами интенсивно изучалась (и в меньшей степени испытывалась) в течение последнего десятилетия. По крайней мере три поставщика – Bloom Energy (США), Doosan (Южная Корея) и SOLIDPower (Германия) – имеют

инсталляции топливных элементов в ЦОДах. Из них наиболее известен успешный проект Bloom Energy с Equinix. Топливные элементы, возможно, являются единственной технологией (помимо генераторов), которая может обеспечить надежную непрерывную генерацию электричества непосредственно на площадке ЦОДа.

Использование топливных элементов для ЦОДов – вопрос спорный и горячо обсуждается. Некоторые, включая активистов из Санта-Клары (шт. Калифорния, США), утверждают, что топливные элементы, как и генераторы, не являются экологически чистыми, поскольку большинство из них используют газ на основе ископаемого топлива (или водород, для получения которого обычно требуется энергия на основе ископаемого топлива). Другие говорят, что использование магистрального или локально хранящегося газа создает риски для надежности и безопасности.

Этим аргументам можно противопоставить довольно высокую надежность систем газораспределения и тот факт, что проблемы безопасности при их эксплуатации возникают довольно редко. Но топливные элементы имеют два других существенных недостатка: во-первых, они стоят больше, чем генераторы, в пересчете на киловатт-час и в основном экономически оправдывают себя только при поддержке соответствующих проектов различными грантами; во-вторых, они требуют постоянной, устойчивой нагрузки (из-за архитектуры топливных элементов). Это приводит к усложнению конструкции и еще большему удорожанию проектов.

Дебаты, конечно, будут еще продолжаться. Но системы на базе топливных элементов, несмотря ни на что, активно разворачиваются: запланированный парк ЦОДов в Коннектикуте (информация о владельце/операторе в настоящее время является конфиденциальной) будет иметь 20-МВт установку на топливных элементах Doosan; Equinix заявляет об увеличении числа установок; Uptime Institute получает информацию и о схожих планах других компаний. Главные причины выбора топливных элементов не связаны с их стоимостью или надежностью, скорее, это возможность добиться резкого сокращения выбросов углекислого газа и других вредных веществ и построить систему, в которой оборудование не будет простаивать.

Идея использования возобновляемых источников энергии на местах в качестве основной системы энергоснабжения ЦОДов пока не получила особой поддержки. Но эксперты Uptime Institute видят набирающую обороты тенденцию: размещение дата-центров рядом с местными источниками энергии, такими как гидроэнергия (или, в теории, биогаз). В Европе рассматриваются по меньшей мере два таких проекта. Такие ЦОДы будут опираться на два отдельных, но локальных источника энергии, что обеспечит теоретическую возможность обслуживания без отключения полезной нагрузки (concurrent maintainability) в случае отказа одного из них. Локальное накопление энергии с использованием батарей и других технологий обеспечит дополнительную безопасность в части энергоснабжения.

Edge-ЦОДы

Средние и крупные дата-центры предъявляют высокие требования к электропитанию, и в большинстве случаев им нужна высокая доступность систем энергоснабжения. Но это не всегда верно для небольших ЦОДов, скажем, с энергопотреблением ниже 500 кВт, которых,

Преимущества	Недостатки
➢ Высокая плотность мощности ➢ Надежный автономный источник электроэнергии ➢ Проверенная временем и множеством проектов технология ➢ Распространенные системы, знакомые многим специалистам ➢ Практически неограниченная подача электричества ➢ Низкие/средние эксплуатационные расходы ➢ Простая синхронизация при подключении в параллель.	➢ Высокий уровень выделений углекислого газа ➢ Высокий уровень выделений твердых частиц ➢ Высокие капитальные расходы ➢ Жесткое регулирование, есть ограничения по эксплуатации ➢ Работают только в аварийных ситуациях, подолгу простаивают ➢ Требуют регулярных проверок и технического обслуживания ➢ Необходимы топливохранилища большого объема на площадке ➢ Требуют много места для размещения ➢ Низкая мобильность, сложно перемещать ➢ Электричество доступно не мгновенно, необходим ИБП.

Источник: Uptime Institute

◀ Преимущества и недостатки дизель-генераторов

как ожидается, в ближайшее десятилетие будет становится все больше. Таким ЦОДам проще обеспечить дублирование ИТ-нагрузки и данных в аналогичных ЦОДах, расположенных поблизости, их проще включить в распределенные системы восстановления, и в любом случае они вызовут меньше проблем, если пострадают от перебоев в подаче электричества.

Но главное здесь то, что такие ЦОДы могут развертывать аккумуляторные батареи (или небольшие топливные элементы) для достижения достаточного времени автономии, перераспределяя трафик и нагрузки по сети при угрозе превышения емкости автономных ресурсов электроэнергии. Например, смонтированная в контейнере система литий-ионных аккумуляторов емкостью 500 кВт·ч может выполнять все функции источника бесперебойного питания, подавать энергию обратно в центральную электросеть и обеспечивать несколько часов работы небольшого ЦОДа (скажем, на 250 кВт) в случае отключения электропитания. По мере совершенствования технологии и снижения цен такие развертывания станут обычным делом. Кроме того, при использовании вместе с небольшим генератором эти системы могут обеспечивать электроэнергию в течение длительного времени.

Отказоустойчивость в облачной среде

Когда представители Microsoft, Equinix и других компаний говорят о снижении зависимости от генераторов, они в основном имеют в виду широкое использование альтернативных источников энергии. Но «Святой Грааль» для операторов гипермасштабируемых ЦОДов и даже меньших кластеров дата-центров – это репликация и управление нагрузкой для быстрой переконфигурации сети ЦОДов, если один из ее элементов начинает испытывать проблемы с электроснабжением.

Такие архитектуры доказывают свою эффективность, но они дороги, сложны и далеко не всегда обеспечивают безотказное предоставление сервисов конечным пользователям. Даже при полной репликации потеря всего ЦОДа не может не вызвать проблем с производительностью. По этой причине все крупные операторы продолжают строить дата-центры с возможностью обслуживания без отключения полезной нагрузки и автономными системами электропитания на площадке.

Изменится ли такое положение дел по мере совершенствования ПО и дальнейшего развития закона Мура? Исходя из текущего состояния отрасли ЦОДов и планируемых новых проектов, ответ будет категорический: «пока нет». Но в 2019 г. по крайней мере один крупный оператор провел испытания, чтобы определить отказоустойчивость своих ЦОДов с использованием описываемых технологий. Вероятная цель будет заключаться не в полном отказе от генераторов, а в сокращении той части рабочей нагрузки, которая потребует резервирования электропитания с помощью ДГУ.

Литий-ионные АКБ и «умная» энергия

Для проектировщиков дата-центров одним из наиболее важных достижений последних лет является «созревание» – технически и экономически – технологии литий-ионных аккумуляторов. С 2010 по 2018 гг. стоимость таких аккумуляторов (в $ за кВт·ч) упала на 85%, по данным Bloomberg NEF (New Energy Finance). Большинство аналитиков ожидают, что цены продолжат неуклонно снижаться в течение следующих пяти лет, причем основной причиной этого будет крупномасштабное производство. Таким образом, создается возможность внедрения новых решений для накопления электроэнергии – в том числе в качестве замены генераторов.

Хотя массовое внедрение литий-ионных аккумуляторов в ЦОДы только начинается, все больше участников рынка – крупных операторов, производителей и стартапов – рассматривают возможность использования литий-ионных хранилищ энергии в сочетании с различными технологиями ее генерации, чтобы уменьшить свою зависимость от традиционных дизель-генераторов. Не стоит рассматривать прямую замену генераторов на литий-ионные накопители, это вряд ли будет экономически выгодно (по крайней мере, в ближайшее время). Скорее речь может идти об использовании таких накопителей в различных схемах совместно с ИБП. Например, реализуя перенос нагрузки и закрытие приложений в соответствии с уровнем их критичности, можно значительно увеличить время автономной работы от ИБП, а значит, позже запускать генераторы (или вовсе от них отказаться). Вероятно, уже в текущем году мы узнаем о пилотных проектах с использованием таких схем.

Вместе с тем уже появились альтернативные технологии, которые могли бы конкурировать с литий-ионными батареями в ЦОДах. Это, например, натрий-ионные батареи на основе электродов, модифицированных берлинской лазурью (Prussian blue). Так что технический прогресс не стоит на месте, и традиционным дизель-генераторам будет все труднее сохранять свое «место под солнцем» на стремительно развивающемся рынке ЦОДов. ИКС

Проектируем систему вентиляции и охлаждения ДДИБП

Намереваясь разместить дизельный динамический ИБП внутри здания дата-центра, оцените варианты такого размещения на ранних этапах предпроекта, не рассчитывая, что этот агрегат и вспомогательные инженерные системы удастся «куда-нибудь запихнуть» позднее.

Андрей Павлов, генеральный директор, «ДатаДом»
Максим Матвиенко, главный инженер проекта, «ДатаДом»

Дизельные динамические (роторные) источники бесперебойного питания (ДДИБП) давно и прочно вошли в российскую практику построения центров обработки данных. Безусловно, у этой технологии есть свои плюсы и минусы, свои сторонники и противники. В этой статье мы не будем обсуждать целесообразность применения ДДИБП на том или ином объекте, а поделимся своим опытом проектирования вспомогательных систем ДДИБП – вентиляции и охлаждения. По большому счету они мало отличаются от аналогичных систем ДГУ, но последние гораздо чаще выпускаются в контейнерном исполнении с индивидуальными, рассчитанными при производстве системами вентиляции и охлаждения и размещаются вне зданий. ДДИБП, как правило, устанавливаются в помещении, зачастую в уже построенном здании, что перекладывает проблему разработки вспомогательных подсистем на плечи проектной организации.

Что должна обеспечить система вентиляции?

Итак, чтобы создать необходимые для работы ДДИБП климатические условия, нужно реализовать системы вентиляции и охлаждения. ДДИБП состоит из двигателя внутреннего сгорания, накопителя и генератора. Все эти элементы при разных режимах своей работы выделяют тепло. Самое большое тепловыделение, до 65% общего выделения ДДИБП, работающего в аварийном режиме, у дизельного двигателя. Поэтому для его охлаждения требуется отдельная система, снимающая излишки тепла с двигателя и выбрасывающая их через радиатор охлаждения. Радиатор может устанавливаться как в одном помещении с ДДИБП, так и вне этого помещения, например, на кровле или за уличной стеной.

Накопитель и генератор создают до 35% общего максимального тепловыделения ДДИБП, но, в отличие от двигателя внутреннего сгорания, делают это при всех режимах работы ДДИБП, а не только при дизельном, как ДВС.

Система вентиляции помещения ДДИБП выполняет три функции: во-первых, утилизирует тепло от корпуса дизельного двигателя, генератора и накопителя, во-вторых, подает кислород для поддержания процесса горения топлива в двигателе и, в-третьих, в случае установки радиатора охлаждения двигателя внутри помещения снимает теплопритоки в дизельном режиме.

При установке радиатора внутри помещения порядка 90% объема воздуха, необходимого в аварийном режиме, затрачивается на съем теплопритоков от всех элементов ДДИБП и порядка 10% расходуется на горение топлива.

В качестве примера приведем статистические данные по системе вентиляции для ДДИБП мощностью 1,6 МВт, которые неоднократно использовались в российских проектах ЦОДов. В одном из реализованных проектов радиатор охлаждения ДВС был установлен внутри помещения рядом с агрегатом ДДИБП, что повысило требования к производительности системы вентиляции. Геометрия помещения обусловила необходимость длинных воздуховодов, вследствие чего мощность приточной установки должна была составлять порядка 100 тыс. куб. м/ч. Расчетное потребление ДДИБП для собственных нужд равнялось 60 кВт, однако реальное пиковое потребление системы вентиляции достигало почти 100 кВт.

Почему возникают сложности?

Основные причины, по которым реализация системы вентиляции ДДИБП вызывает сложности в российских дата-центрах, – это сезонные перепады температур и часто практикуемое размещение данного оборудования в здании ЦОДа по остаточному принципу. В штатной комплектации радиатор охлаждения и

Рис. 1.
Типовая компоновка ДДИБП и системы охлаждения ▶

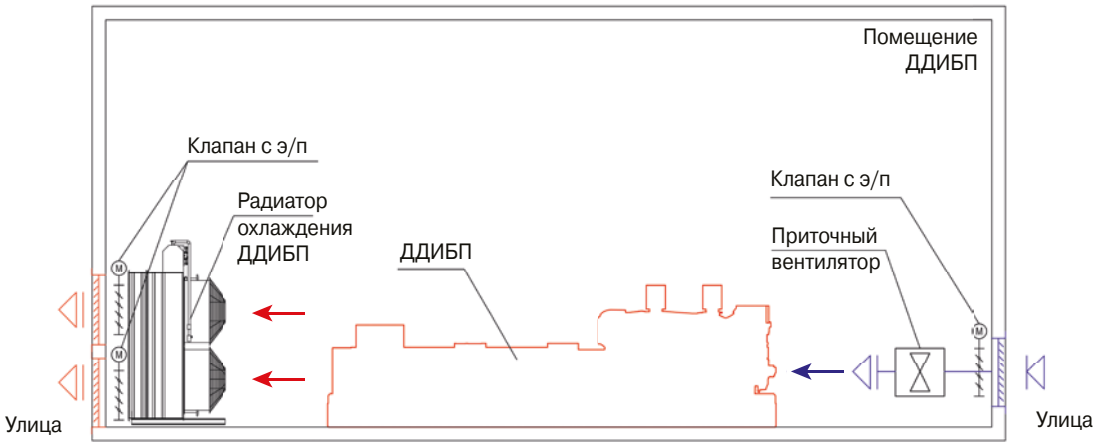
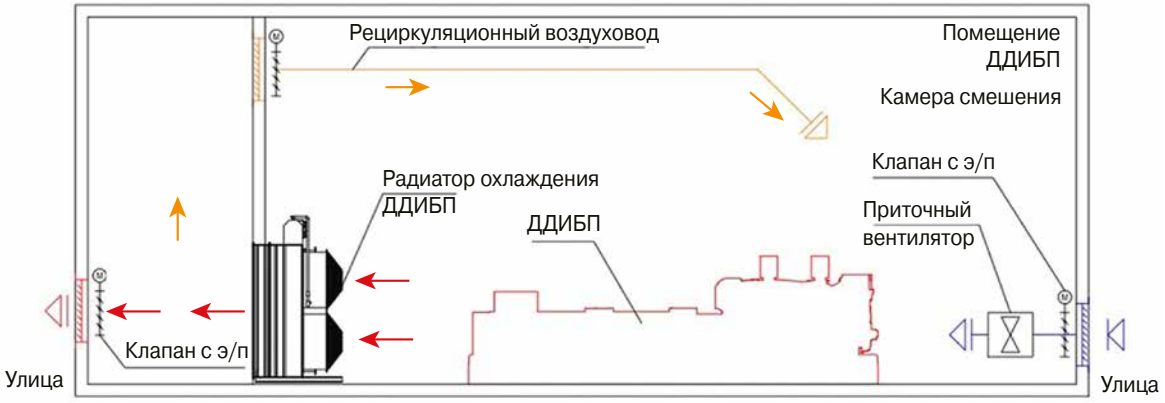


Рис. 2.
Установка ДДИБП с камерой смешения воздуха ▶



двигатель ДДИБП способны принимать уличный воздух температурой до –15°С. В большинстве европейских стран такой мороз – минимальная сезонная температура. Поэтому в стандартной схеме ДДИБП располагается в здании с организацией забора воздуха со стороны генератора напрямую с улицы, движением его вдоль установки, с одновременным забором тепловыделений генератора, накопителя и двигателя, и последующим выбросом воздуха через радиатор охлаждения на улицу с другой стороны здания (рис. 1).

В России такая компоновка в большинстве случаев нереализуема из-за ограничений на температуру подаваемого на установку наружного воздуха. При допустимых паспортных –15°С температура в наших краях может быть существенно ниже и опускаться до –40°С, что заставляет создавать камеру смешения воздуха. Это увеличивает как капитальные вложения (а заодно и требуемые размеры помещения для ДДИБП), так и операционные расходы, в частности, на электроснабжение и эксплуатацию дополнительных вентиляционных групп.

Камерой смешения может служить непосредственно помещение, где установлен ДДИБП (рис. 2). В этом помещении устанавливаются два воздушных клапана с электроприводом, соединяющих его с улицей и отсеком рециркуляции. Открывая и закрывая клапаны, можно регулировать количество нагретого воздуха, подаваемого обратно в помещение ДДИБП через рецикуляционный воздуховод.

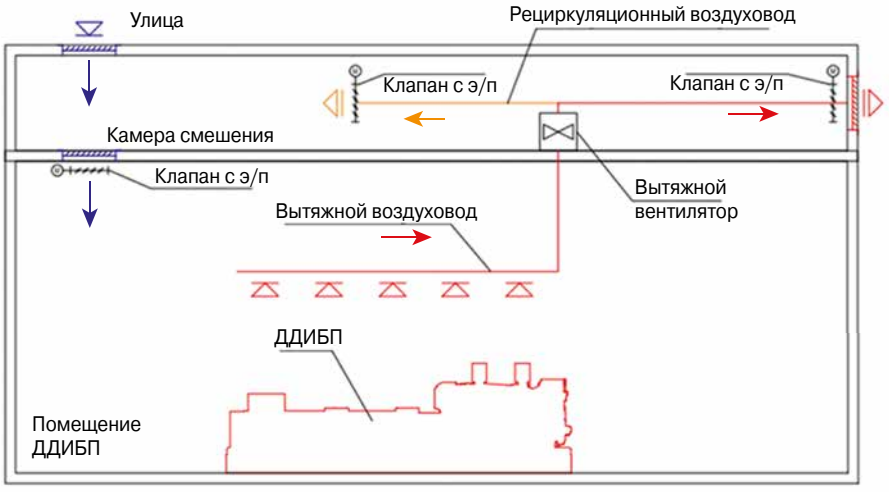
Если температура в помещении ДДИБП снижается, приточный клапан начинает закрываться (при этом снижаются обороты приточного вентилятора), одновременно с этим закрывается вытяжной клапан. Рециркуляционный клапан открывается, подмешивая нагретый воздух после радиатора охлаждения обратно в помещение (где он смешивается с наружным воздухом). Если температура внутри помещения растет, то происходит обратный процесс – клапаны наружного и вытяжного воздуха начинают открываться, а рециркуляционный клапан закрывается. Комбинация этих режимов работы позволяет поддерживать требуемую температуру внутри помещения ДДИБП.

На деле мы часто ограничены геометрией здания, его внешним окружением, пожеланиями заказчика, поэтому приходится создавать более сложные системы вентиляции.

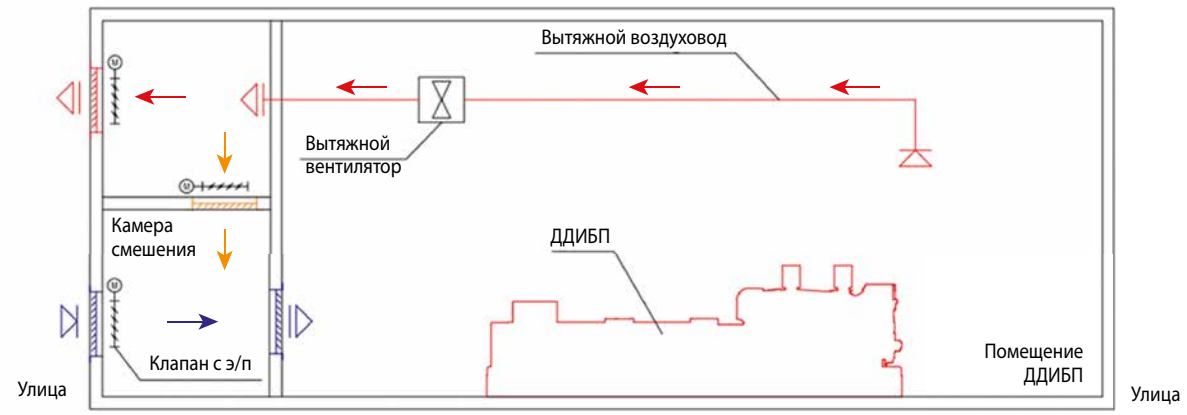
Что получается на практике?

Так, на одном из проектируемых объектов отсутствовала возможность установить клапаны

забора и выброса воздуха с фасада здания на расстоянии более 6 м друг от друга (для исключения их взаимного влияния), однако можно было обеспечить забор воздуха с кровли. В результате родилась схема, представленная на рис. 3. Радиатор ДДИБП размещался на улице, на специальной эстакаде. Установка радиатора вне помещения позволила снизить нагрузку на систему вентиляции, поскольку отпала необходимость подавать в помещение дополнительный объем наружного воздуха для охлаждения ДДИБП. Кроме того, расположение воздухозабора на кровле существенно снизило скорость загрязнения воздушных фильтров.



▲ **Рис. 3. Организация забора и выброса воздуха для охлаждения ДДИБП с кровли здания**



◀ **Рис. 4. Конфигурация со свободным размещением вытяжного вентилятора**

Камера смешения фактически представляла собой дополнительный технический этаж, находящийся над помещением ДДИБП. Это позволило уменьшить размеры помещения ДДИБП за счет выноса части вспомогательных систем за его пределы. Установка вытяжных вентиляторов в отдельном помещении упростила обслуживание системы вентиляции (замену фильтров, ремонт и замену неисправных вентиляторов) и дала больше свободы при размещении шумоглушителей в помещении ДДИБП.

Такая компоновка позволила снизить требуемую протяженность помещения, но его высота существенно увеличилась по сравнению с предыдущим вариантом. Недостатки решения – большое количество поворотов потока воздуха, повысившее энергопотребление системы вентиляции, а также нехватка места для свободного размещения вытяжных вентиляторов, что заставило уделить особое внимание расчету необходимой производительности последних во избежание их работы в критичных режимах.

Топология еще одного объекта позволяла сделать забор и выброс воздуха только на стене помещения ДДИБП, граничащей с улицей. При этом на площадке не было возможности проложить вытяжные шахты внутри здания. Радиатор охлаждения также был вынесен за пределы здания (рис. 4).

Эта компоновка также отличается повышенным энергопотреблением, обусловленным сложным маршрутом движения воздушных потоков, и наибольшей высотой помещения среди всех рассмотренных вариантов. Высота помещения определяется габаритами вентиляционных решеток и строительными нормами на расстояние между ними и для ДДИБП мощностью 1,9 МВт составляет не менее 11 м. Но в данном случае вытяжные вентиляторы можно было расположить свободно, что позволило подобрать оборудование с необходимым запасом мощности.

Приведенные примеры наглядно демонстрируют, что размещение ДДИБП внутри здания – задача нетривиальная. Поэтому мы настоятельно рекомендуем оценивать возможные варианты расположения данного оборудования в здании ЦОДа еще на самых ранних этапах предпроектных работ, не рассчитывая на то, что ДДИБП и все вспомогательные инженерные системы удастся «куда-нибудь запихнуть» в уже отрисованную архитектуру здания на более поздних этапах проектирования. ИКС

Тонко о распыленной воде

Установка пожаротушения HI-FOG® производства компании Marioff – основа многоступенчатой системы обеспечения пожарной безопасности дата-центров IXcellerate.

Сергей Вышемирский, технический директор, IXcellerate

Василий Углов, технический директор, Marioff Russia

Надежность на высоком уровне

IXcellerate – это ведущий оператор коммерческих центров обработки данных, входящий в топ-3 крупнейших игроков России. Первый машинный зал – IXcellerate Moscow One – был введен в эксплуатацию в 2013 г., и его вместимость составляет 1835 стойко-мест. Второй дата-центр, IXcellerate Moscow Two, введен в эксплуатацию в 2019 г. с показателем 1480 стойко-мест. Оба дата-центра нейтральны, сертифицированы IBM и Uptime Institute и соответствуют уровню надежности Level 3/Tier III. Доступность сервиса гарантируется на уровне 99,999%.

Все инженерные системы дата-центров IXcellerate спроектированы для обеспечения повышенной надежности. Резервирование внешнего электроснабжения внутри площадки по схеме «ИБП + ДГУ», высокоэффективные ИБП с двойным преобразованием и модульной конструкцией, использование современных литий-ионных батарей позволяют гарантировать ключевой параметр надежности дата-центра – непрерывность электроснабжения. Кросс-коммутация, нейтральное подключение к любому из 51 оператора связи, применение технологии 2 Meet-Me-Room обеспечивают высокую коннективность. Системы физической защиты, интеллектуальной безопасности и технической поддержки в режиме 24/7 страхуют от возможных неожиданностей.

Однако не только отказы электроснабжения, обрывы связи или хакерские атаки могут прервать доступность сервисов дата-центра для клиентов. Пожар – чрезвычайно опасная ситуация, редкая, но чреватая тяжелейшими последствиями. Специалисты компании Capitoline (www.capitoline.org) изучили 219 случаев полного отказа оборудования дата-центров с суммарным временем простоя 2074 часа. Среднее время простоя оборудования из-за отказов электроснабжения составляет 6,5 часа, из-за программных сбоев – 16,7 часа, из-за ложных срабатываний установок пожаротушения – 17,1 часа... и 25 часов – в случае пожара! Восстановить нормальную работу дата-центра после пожара – очень сложная задача, ведь, по данным того же исследования, большинство дата-центров не имеют плана восстановления работоспособности в ходе такого сценария.

Команда IXcellerate готова к любым неожиданностям. Пожарная безопасность дата-центров IXcellerate Moscow

One и Moscow Two обеспечивается многоступенчатой системой мер, включающей в себя тщательный подбор материалов и оборудования, инженерные системы противопожарной защиты и организационные мероприятия. Такой комплексный подход позволяет реагировать на любой сценарий развития событий гибко, оперативно и эффективно, сочетая оптимизацию затрат и высокий уровень безопасности.

К пожару готовы

Аспирационные установки пожарной сигнализации (в Moscow One используется Vesda, а в Moscow Two – Wagner) в непрерывном режиме отбирают пробы воздуха из множества точек защищаемого помещения и анализируют их при помощи интеллектуальных датчиков. Это обеспечивает сверхбыстрое обнаружение пожара – датчики срабатывают в момент появления в воздухе первых следов продуктов термического разложения горючих материалов – еще до появления видимого дыма. Система определяет место возникновения горения и адаптируется к разным уровням запыленности и влажности воздуха. Это позволяет персоналу реагировать на возникшую ситуацию почти мгновенно.

Независимо от системы пожарной сигнализации действует автоматическая установка пожаротушения. Здания дата-центров целиком защищены установками пожаротушения тонкораспыленной водой HI-FOG® производства финской компании Marioff. Принцип действия установки – распыление водяного тумана под высоким давлением – позволяет совместить преимущества водяных и газовых установок пожаротушения. Скоростные струи из мельчайших водяных капель сбивают пламя, перемешивают объем зоны горения, насыщая ее водяным паром, резко охлаждают зону пожара и мгновенно приводят значения температуры в защищаемом помещении к нормальному уровню. Тонкая водяная пыль, висящая в воздухе вокруг зоны горения, блокирует тепловое излучение, защищает соседнее оборудование и конструкции здания от прогрева и надежно останавливает распространение пожара. При этом тонкораспыленная вода не требует герметичности защищаемого объема – в отличие от установок газового пожаротушения – и обеспечивает надежное тушение при различных скоростях движения воздуха.

Патентованные спринклерные распылители HI-FOG® оснащены термочувствительными колбами, срабатывающими при определенной температуре, – это дает возможность распылять воду только там, где необходимо, в отличие от газовых установок пожаротушения, требующих заполнения всего объема машинного зала огнетушащим веществом. В дата-центрах IXcellerate Moscow One и Moscow Two применяется спринклерно-дренчерная конфигурация установки пожаротушения (технология DOUBLE-INTERLOCK PREACTION), позволяющая свести к нулю вероятность ложного срабатывания. Трубопроводы установки заполнены сжатым воздухом, вода в дежурном режиме в трубопроводы не подается. Узел управления контролирует давление сжатого воздуха в трубопроводной сети, к которой присоединены спринклерные распылители, запертые

термочувствительными колбами. При получении сигнала «Пожар» от датчиков пожарной сигнализации узел управления переключается в режим готовности к тушению, но подачи воды в секцию не происходит. Как только первый из распылителей – ближайший к месту пожара – прогреется до нужной температуры, колба лопнет, давление воздуха в трубопроводе упадет и узел управления откроет подачу воды на тушение. Облако из тонкораспыленной воды накроет зону возгорания, собьет пламя и блокирует развитие пожара, охлаждая колбы соседних распылителей. Это минимизирует количество распыляемой воды, она применяется только там, где это необходимо.

Таким образом, для подачи воды на тушение нужно одновременное наступление двух событий – получение сигнала «Пожар» от пожарных датчиков и прогрев колбы распылителя. Это позволяет свести к нулю вероятность ложного срабатывания – если от пожарных датчиков будет получен ложный сигнал (из-за электрических помех, запыленности или по другим причинам), установка пожаротушения перейдет в режим «Пожар», но вода для тушения пожара распылять не начнет, так как термочувствительные колбы распылителей останутся целыми. Если же колба какого-либо распылителя случайно будет разбита (например, при проведении ремонтных или монтажных работ), распыления воды так же не произойдет: узел управления подаст сигнал о падении давления сжатого воздуха в секции, но подача воды

в трубопровод останется закрытой – ведь пожарная сигнализация не активировала сигнал «Пожар».

В качестве основного источника огнетушащего вещества используются емкости с дистиллированной водой, которая является диэлектриком и оказывает минимальное воздействие на серверное оборудование. Резервным источником огнетушащего вещества служит вода из системы Мосводоканала.

В дополнение к высокочувствительной интеллектуальной сигнализации и высоконадежной, инновационной установке пожаротушения помещения дата-центров оснащены ручными газовыми огнетушителями, которые позволяют персоналу, прибывшему на место происшествия, уверенно тушить возгорания в начальной фазе их развития без отключения работающего оборудования, не опасаясь коротких замыканий.

Преимущества для клиентов

Таким образом, правильный подбор систем обеспечения пожарной безопасности и организационных мер позволяет максимально использовать преимущества современных технологий и при этом компенсировать их возможные слабости. Однако в процессе принятия решений по противопожарной защите удалось добиться не только надежности и безопасности, но и значительной экономической оптимизации – и некоторых принципиальных преимуществ для клиентов дата-центров IXcellerate.

В частности, применение установки пожаротушения тонкораспыленной водой вместо газовой установки пожаротушения позволило отказаться от деления машинного зала на несколько изолированных помещений. Это дало возможность разместить в двух центрах обработки данных почти на 400 стойко-мест больше – при сокращении капитальных затрат на строительные работы и инженерные системы.

Еще одно неочевидное эксплуатационное преимущество такой схемы становится ключевым для нейтрального дата-центра, работающего по схеме colocation. Огромная площадь машинного зала позволяет предложить заказчикам размещение их оборудования на любой площади, которая им необходима, – выделяя нужную зону временными перегородками, оборудуя ее системами контроля доступа, видеонаблюдения и другой аппаратурой по желанию заказчика. Это преимущество чрезвычайно важно для крупных клиентов – к тому же такое решение является очень гибким, позволяя при необходимости быстро и недорого менять конфигурацию машинного зала, адаптируя его под требования новых заказчиков.

Высокие эксплуатационные характеристики установки пожаротушения HI-FOG® помогают оптимизировать ее обслуживание – такая установка не требует регулярной замены огнетушащего вещества, перезарядка после срабатывания практически ничего не стоит, а расчетный срок службы установки превышает 40 лет. Трубопроводы и фитинги из высококачественной нержавеющей стали, насосы специальной конструкции и надежные резьбовые соединения позволяют свести трудозатраты на обслуживание установки к минимуму, обеспечивая при этом высокую надежность работы в течение десятилетий.

Неудивительно, что при расширении эксплуатационных мощностей – строительстве новых дата-центров IXcellerate Moscow Three и Moscow Four – на новых площадках планируется применить те же опробованные, проверенные временем технические решения.

Сотрудничество компаний IXcellerate и Marioff продолжается. В конце концов, у нас общие цели – безопасность бизнеса наших клиентов.

IoT в зданиях: требуется единая сеть доступа

При развертывании решений IoT в коммерческих зданиях компании сталкиваются со сложной, фрагментированной экосистемой стандартов, устройств и технологий. Эта сложность часто замедляет или останавливает проекты IoT из-за неопределенности возврата инвестиций.

Дмитрий Оськин, технический эксперт, CommScope

Сегодня в комплексных проектах автоматизации зданий число устройств IoT – различных датчиков, маяков, исполнительных механизмов и т.д., подключаемых по беспроводным каналам, растет лавинообразно. Для их подключения могут служить технологии Bluetooth Low Energy (BLE), Zigbee, RFID, NFC, LoRa, NB-IoT, LTE cat. M и др. Без тщательного планирования (и эффективной интеграции) результатом такого подключения будет большое количество наложенных сетей и дублирование оборудования (кабельных систем, коммутаторов и пр.), средств обеспечения безопасности, систем мониторинга и управления. Подобная избыточность усложняет и удорожает проекты.

Кроме того, различные беспроводные технологии зачастую используют один частотный диапазон, что приводит к межканальным помехам, затрудняющим работу систем и приложений.

Основные технологии

Для подключения устройств IoT задействуется множество беспроводных технологий. Они существенно различаются по радиусу действия (площади покрытия) и скорости передачи данных (рис. 1), а также по специфике применения. К числу наиболее популярных относятся BLE, Zigbee и LPWAN (см. таблицу).

Технология Bluetooth хорошо известна даже неспециалистам, поскольку она реализована во всех современных смартфонах. Изобретенная в начале 90-х годов в Ericsson, Bluetooth была в 2002 г. стандартизована институтом IEEE в документе 802.15.1. Позже IEEE отказался от стандарта, и в настоящее время технология поддерживается организацией Bluetooth Special Interest Group.

Устройства Bluetooth работают в частотном диапазоне от 2,4 до 2,485 ГГц (рис. 2). Существует два основных варианта этой технологии:

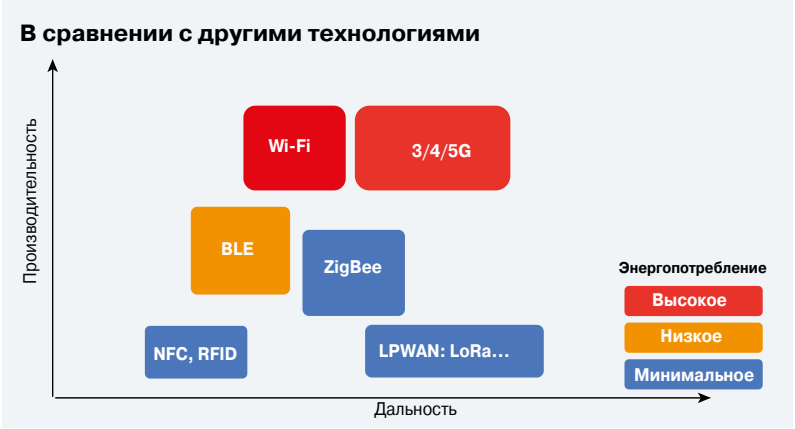


Рис. 1. Технологии, используемые для подключения устройств IoT ▼

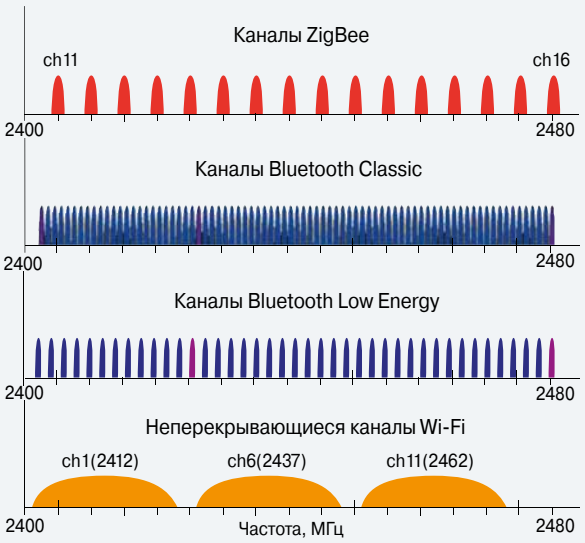


Рис. 2. Частотные каналы, используемые Bluetooth, Bluetooth Low Energy, ZigBee и Wi-Fi ▶

Bluetooth Classic (1.x, 2.x) и Bluetooth Low Energy (BLE Smart, BLE 4.x, BLE 5.0). В обоих вариантах используется псевдослучайная перестройка рабочей частоты. Данные делятся на пакеты и в случае Bluetooth Classic передаются по одному из 79 каналов шириной 1 МГц каждый, а устройства Bluetooth Low Energy задействуют 40 каналов по 2 МГц. Сейчас в основном применяется вариант BLE.

Технология Bluetooth часто используется в так называемых маяках (beacon). Маяки отслеживают местоположение устройств с поддержкой этой технологии и при их приближении запускают приложения, которые передают на устройства данные, имеющие отношение к конкретному месту, например, информацию об акциях близлежащего магазина. Основные протоколы для маяков предлагают Apple и Google.

Apple iBeacon – встроенный в iOS 7 протокол, который позволяет устройствам iPhone/iPad постоянно сканировать маяки BLE. Google Eddystone, ранее называвшийся UriBeacon, представляет собой протокол для маяков с открытым исходным кодом, которые могут быть изготовлены кем угодно. Ряд производителей маяков, например компания Kontakt.IO, поддерживают оба протокола, iBeacon и Eddystone, а также предлагают собственные протоколы для передачи телеметрических данных со своих маяков и тегов.

Zigbee – это спецификация на основе стандарта IEEE 802.15.4 для набора высокоуровневых протоколов связи, поддерживаемых группой Zigbee Alliance. Технология предназначена для маломощных устройств с низкой пропускной способностью, которые обычно служат для сбора данных домашней автоматизации и медицинских данных. Работает на частоте 2,4 ГГц, но также может задействовать частоты 784 МГц (в Китае), 868 МГц (в Европе) и 915 МГц (в США и Австралии). Сетевой уровень Zigbee изначально поддерживает топологии «звезда» и «дерево», а также ячеистые (mesh) сети. С 2006 г. спецификация Zigbee предлагает полное взаимодействие между устройствами производителей, использующих библиотеку кластера Zigbee.

Устройства с поддержкой Zigbee – одни из самых популярных в мире IoT. Они широко применяются в системах измерения и индикации, «умного» освещения, отопления, вентиляции и кондиционирования, различных интеллектуальных замках, системах охраны и безопасности.

В семейство LPWAN входят различные технологии для территориально распределенных сетей (WAN) с низким энергопотреблением конечных устройств (Low Power, LP). Эти сети работают как в лицензируемом (NB-IoT и LTE cat. M), так и в нелицензируемом частотных диапазонах. К наиболее распространенным системам, которые используют нелицензируемые частоты, относятся системы LoRa (что означает Long Range). Все решения LPWAN характеризуются:

- большим радиусом действия (несколько километров в городе, десятки километров вне города);
- низким энергопотреблением конечных устройств;
- низкой скоростью передачи данных (несколько килобит в секунду).

Типичное применение технологий LPWAN – подключение счетчиков ЖКХ. Чтобы собирать информацию о потреблении воды, электричества и газа, достаточно передавать данные один раз в день или даже в несколько дней.

Технология	Сравнительное потребление энергии	Стоимость	Скорость	Шифрование	Радиус действия
Bluetooth	Низкое	Низкая	2 Мбит/с	Есть	40 м
Zigbee	Очень низкое	Низкая	0,25 Мбит/с	Есть	20 м
Wi-Fi	Высокое	Средняя	50+ Мбит/с	Есть	50 м
LPWAN (LoRa)	Самое низкое	Низкая	До 40 кбит/с	Есть	До 2 км в городе До 20 км вне города

Источник: CommScope

На пути к единой инфраструктуре

В идеале все эти сети должны быть способны работать в одной конвергентной инфраструктуре. В зданиях такое объединение оптимально реализовать на базе хорошо знакомых корпоративным заказчикам сетей Wi-Fi. Вместо того чтобы пытаться управиться с «зоопарком» из не-

скольких различных новых инфраструктур, нужно иметь возможность использовать архитектуры управления и безопасности, действующие в сети Wi-Fi, для всех беспроводных устройств IoT независимо от радиотехнологии их подключения. При этом важно иметь единый интерфейс управления как беспроводным сегментом сети (точками доступа), так и проводным сегментом (коммутаторами и контроллерами точек доступа), что сделает мониторинг и управление всей сетью удобным и прозрачным.

Конвергентная сеть доступа IoT должна максимально использовать уже имеющиеся проводные и беспроводные сетевые инфраструктуры. Это позволит задействовать существенно меньше портов коммутаторов, а также сократить число элементов кабельных систем, обеспечив значительную экономию средств. Физическая инфраструктура станет не только дешевле, но и проще, что облегчит эксплуатацию и повысит надежность.

Как создать такую конвергентную сеть? Один из вариантов – наделить точки доступа Wi-Fi средствами поддержки других радиотехнологий, используемых устройствами IoT, например, широко распространенных BLE и Zigbee. Такая поддержка может быть реализована как непосредственно в платах точек доступа Wi-Fi, так и с помощью устанавливаемых в них дополнительных модулей. Это превратит точки доступа Wi-Fi в интегрированные узлы с функционалом соответствующих шлюзов – BLE или Zigbee.

Ряд новейших моделей точек доступа, которые работают по технологии 802.11ax (Wi-Fi 6), благодаря наличию внешних USB-адаптеров можно считать конвергентными устройствами, способными обеспечить совместимость с новыми беспроводными технологиями (которые уже разработаны или появятся в будущем). Например, с помощью установки внешнего USB-модуля можно реализовать поддержку радиопротокола Z-Wave, широко используемого сейчас в системах домашней автоматизации.

Поддержка Wi-Fi, BLE и Zigbee одним узлом также поможет минимизировать помехи в сильно загруженном диапазоне 2,4 ГГц, в котором работают все эти технологии (см. рис. 2). Такая минимизация требует специальных мер на всех уровнях. На физическом уровне это можно сделать на этапе проектирования конвергентных точек доступа с использованием встроенных механизмов чипов. На более высоких уровнях могут применяться специализированные программные алгоритмы и технологии. Также следует задействовать специальные средства организации радиоканалов, радиопланирования и пр.

Если на начальном этапе поддержка той или иной радиотехнологии в едином узле доступа не оправдана технологически или экономически, можно обеспечить единое управление на уровне контроллера. Например, для работы с технологией LoRa в контроллер IoT можно встроить центральный сервер сети LoRaWAN, который будет принимать решения о необходимости изменения скорости передачи данных конечными узлами, мощности передатчика, о выборе канала передачи, ее начале и продолжительности, контролировать заряд батарей конечных узлов, т.е. полностью контролировать сеть и управлять каждым абонентским устройством в отдельности. Помимо преимуществ общего управления такой подход обеспечит единую точку интеграции для сопряжения с другими системами, что чрезвычайно важно для развития приложений и сервисов IoT. Подключать такие сервисы можно через открытый прикладной интерфейс (Open API) контроллера IoT.

Еще одно преимущество конвергентной сети доступа для IoT-устройств, работающих по разным радиотехнологиям, – возможность построения эффективной системы безопасности с единой политикой. При реализации подобной системы важен комплексный подход, обеспечивающий физическую безопасность, эффективную идентификацию и аутентификацию конечных устройств (например, с использованием цифровых сертификатов), а также шифрование и изолирование трафика. В частности, для точек доступа IoT и контроллера целесообразно использовать отдельную виртуальную локальную сеть (VLAN), а весь не-IoT трафик держать в другом месте – например, для трафика Wi-Fi выделить свою сеть VLAN.

По мере того как к сети будет подключаться все больше и больше устройств IoT, традиционная инфраструктура WLAN или LAN будет дополняться или заменяться с целью построения универсальной сети доступа, которая соединит все устройства IoT в пределах ограниченной территории, такой как университетский кампус или офисное здание. Сеть доступа IoT объединит несколько сетей физического уровня в единую конвергентную сетевую инфраструктуру. Эта общая сеть упростит подключение устройств IoT, установит единые протоколы безопасности, объединит управление такими устройствами и настройку политик.

Создание сетей доступа IoT на основе имеющейся инфраструктуры LAN и WLAN сократит время развертывания, упростит и унифицирует мониторинг и управление сетью за счет единого интерфейса управления беспроводными точками доступа и проводными коммутаторами. В результате снизятся затраты на поддержку нескольких решений IoT, что позволит строить решения, конкурентоспособные как по техническим, так и по экономическим показателям. ИКС

ИБП: время обновления

Schneider Electric проводит масштабное обновление линейки ИБП. В приоритете – энергоэффективность, модульность, компактность, использование литий-ионных АКБ. Подробнее – Павел Пономарев, менеджер по развитию направления «Трехфазные ИБП» подразделения Secure Power.

– Павел, как сегодня меняются запросы заказчиков на системы бесперебойного питания?

– При разработке инженерной инфраструктуры в целом заказчики стали более тщательно рассчитывать первоначальные затраты, стараются снизить CAPEX. Проекты, в которых используются трехфазные ИБП средней и большой мощности, обычно «долгоиграющие», и мы сталкиваемся с ситуациями, когда бюджет на проект планировался несколько лет назад и теперь пересматривается в меньшую сторону. Это связано и с колебаниями курса рубля, и с переоценкой заказчиком своих потребностей. Компании стали чаще приобретать оборудование исключительно для решения текущих задач, без закладки резерва на будущий рост.

Сложившаяся в мире ситуация негативно повлияла на активность заказчиков. Во втором квартале это ощутили все поставщики. Сейчас заметно оживление, надеемся на восстановление рынка к концу года.

– Предлагаете ли вы какие-либо варианты, позволяющие снизить расходы заказчика на новый ИБП?

– Популярны наши сервисные услуги обновления парка оборудования, в рамках которых заказчик меняет установленные системы на новые со скидкой. Для некоторых типов оборудования, проработавшего 10–15 лет, мы предлагаем полную замену всех внутренних блоков, всего того, что имеет ограниченный ресурс. И это оказывается для компании гораздо выгоднее, чем приобретать новое оборудование.

– А экономия за счет повышения энергоэффективности? Что здесь могут предложить ИБП?

– За последние 10–15 лет КПД современных ИБП серьезно вырос. Во-первых, элементная база стала совершеннее. Произошел отказ от трансформаторов в ИБП благодаря появлению мощных силовых транзисторов. Постоянно улучшаются их характеристики: уменьшаются потери во включенном состоянии и во время переходных процессов, следовательно, повышается КПД.

Во-вторых, развивается схемотехника. Мы в Schneider Electric не просто собираем ИБП на современной элементной базе по старым схемам, как делают многие наши конкуренты, а активно разрабатываем новые. Так, нами запатентованы новые схемы четырехуровневого инвертора (он используется в больших системах Galaxy VX) и трехуровневого инвертора с технологией soft switch, т.е. программным управлением переключением со снижением потребления (этот инвертор используется в новой линейке ИБП Galaxy VS).

Все эти инновации позволяют достичь впечатляющих значений КПД. Например, у ИБП семейства Galaxy VS этот показатель в режиме двойного преобразования превышает 97%. Еще выше КПД в режиме экономии электроэнергии, который в нашем оборудовании называется ECOnversion™ и имеет ряд преимуществ: нулевое время перехода, отсутствие переходных процессов, активная фильтрация помех и т.д. Кроме того, в этом режиме имеется возможность подзаряжать АКБ.

– Большинство ваших новых продуктов выходят в модульном исполнении. Это новый тренд, запросы заказчиков или просто дополнительный способ позиционировать себя относительно конкурентов?

– Это важный тренд. Напомню, что первые модульные ИБП были разработаны и запатентованы компанией APC еще в начале 2000-х гг. Сейчас срок патентов истек, и почти у каждого производителя есть решения, которые они называют модульными.

Все больше заказчиков ориентируются на модульные ИБП, поскольку они обеспечивают удобство обслуживания и дополнительную отказоустойчивость. Такие ИБП позволяют создавать решения со встроенным резервированием без необходимости устанавливать параллельно несколько аппаратов – и тем самым снижать CAPEX.

Хочу отметить, что совсем недавно, в конце июля, линейка наших недорогих ИБП Easy UPS пополнилась мощными моделями на 500 и 600 кВт, которые тоже представляют собой модульные решения. Таким образом модульность, которая изначально появилась в премиальной серии Symmetra и затем была реализована в оптимальной серии Galaxy V (VS, VM, VX), теперь есть и в серии Easy. В модульном исполнении в ней сейчас выполнены решения от 60 до 600 кВт.

Модульность реализована и в ИБП меньшей мощности, например, в линейке Galaxy VS представлены модульные аппараты от 10 до 150 кВт. В них применяются модули, рассчитанные на максимальную мощность 50 кВт, но при отгрузке заказчику они программно прошиваются на необходимую мощность. Если это ИБП на 10 кВт, то и модуль программируется на 10 кВт. В конце сентября, следуя многочисленным пожеланиям заказчиков, мы расширим данную линейку масштабируемой версией ИБП, давая возмож-

ность изменять мощность ИБП самостоятельно путем добавления или убавления модулей мощностью 50 или 20 кВт.

– Вы первыми предложили ИБП с литий-ионными АКБ. Как развивается это направление?

– Сегодня очень важный вопрос – начальная стоимость. Есть разные методы подсчета, но, если сравнивать «яблоки с яблоками» – одинаковые условия мониторинга, время автономии и т.д., – то покупка литий-ионных АКБ обходится дороже, чем свинцово-кислотных. Если говорить о TCO, то ЛИ АКБ становятся более выгодными при горизонте планирования пять-шесть лет и более, т.е. когда приходит время замены свинцово-кислотных батарей. Но в нынешних условиях российские заказчики часто ориентируются на меньшие сроки окупаемости, на два-три года. Да и пандемия внесла коррективы: все интересуются решениями, сбалансированными по стоимости «здесь и сейчас». Это сдерживает рост внедрения ЛИ АКБ.

Но в целом спрос на литий-ион, конечно, растет. На сегодня в мире у нас с ЛИ АКБ работают ИБП суммарной мощностью 1,5 ГВт. Это уникальный опыт. Планируем развивать портфель решений с литий-ионными АКБ. В настоящее время мы предлагаем только один тип ЛИ АКБ: батареи Samsung, построенные по технологии LMO/NMC. Подобные АКБ предлагает и ряд наших конкурентов. Некоторые заказчики запрашивают альтернативные решения, в частности, построенные по технологии LFP, и мы планируем в следующем году тоже выпустить такой продукт, что разнообразит наше предложение и обеспечит заказчикам возможность выбора технологии литий-ионных АКБ.

– Обращение к технологии LFP связано с ее большей безопасностью?

– Часто слышу о том, что LFP-батареи более безопасны. Утверждающие это оперируют известными данными с сайта batteryuniversity.com. Но там приведено академическое исследование. На самом деле важно сравнивать ячейки конкретных производителей. Каждый вендор может добавлять средства безопасности. Так, у батарей Samsung есть и пассивный слой, которые останавливает химическую реакцию при критическом нагреве, и встроенная аппаратная защита от перезаряда (если напряжение на ячейку превышает критический диапазон, срабатывает защита, цепь размыкается и процесс заряда останавливается), и встроенный предохранитель. Поэтому, если рассматривать конкретные реализации, батареи LMO/NMC и LFP имеют одинаковый уровень безопасности.

Наше обращение к технологии LFP связано с другим. Сейчас мы используем ячейки большой емкости, которые были апробированы на электромобилях премиум-класса, в частности BMW. Если мощность, например, edge-ЦОДа составляет 10–20 кВт, то один наш комплект таких батарей обеспечит более часа автономной работы. Это нужно далеко не всегда, обычно достаточно 15–30 минут. Получается, что мы переразмериваем решение, что увеличивает его стоимость. Обращаясь к линейке LFP, мы сможем предложить батареи в том числе меньшей емкости для небольших объектов.

– Для каких проектов литий-ионные АКБ наиболее востребованы?

– Нет какого-либо одного направления, куда ЛИ АКБ можно «грузить пароходами». Все индивидуально, зависит не только от типа, но и от особенностей объекта. На некоторых объектах свинцово-кислотные АКБ физически нельзя ставить, поскольку перекрытие не выдержит, а другое помещение заказчик выделить не может.

В ряде случаев проекты с ЛИ АКБ могут окупиться быстрее, чем за пять-шесть лет, поскольку высвобожденные (в случае замены СК АКБ на ЛИ АКБ) площади можно использовать для размещения дополнительных ИТ-стоек, и если это коммерческий ЦОД с услугами colocation, то он заработает дополнительные деньги. Но бывают ситуации, когда под батареи выделено специальное помещение, и даже если оно будет заполнено только на треть, ИТ-стойки заказчик там все равно установить не сможет. Тогда компактность литий-иона окажется невостребованной.

– Но в целом компактность решения важна для заказчика при выборе оборудования?

– Компактность часто имеет ключевое значение. Например, когда выделенного помещения не хватает, чтобы разместить желаемое оборудование. Такая ситуация может возникнуть, например, при модернизации корпоративных ЦОДов, когда оборудование большей мощности необходимо разместить в изначально выделенном помещении. Часто помещение для ИБП выделяют по остаточному принципу, и туда громоздкое оборудование просто не поставить.

Замечу, что уменьшению размеров наши разработчики уделяют много внимания. Так, уже упомянутый модульный ИБП Easy UPS 3L мощностью 0,6 МВт имеет ширину 1 м, глубину 85 см и стандартную высоту 1,9 м. Это очень компактный аппарат.

Отдельный разговор про малые ЦОДы, в том числе edge-решения. У нас в портфеле есть edge-ЦОД, выполненный в виде небольшого настенного шкафа. В него устанавливается однофазный ИБП с литий-ионными АКБ. Здесь компактность и небольшой вес таких АКБ принципиальны. Это позволяет разместить в небольшом настенном шкафу средства обеспечения времени автономной работы, достаточного для завершения бизнес-приложений.

Мы начали применять ЛИ АКБ с мегаваттными системами. Сейчас расширяем использование таких батарей на небольшие однофазные ИБП мощностью от 1 до 5 кВт. При появлении LFP-батарей закроем диапазон выше 5 кВт – до 30–40 кВт, чтобы обеспечить разумное небольшое время автономии и оптимизировать стоимость.

Инфраструктура ЦОДов в эпоху IoT и Big Data

Николай Ефимов, технический менеджер, Siemon

Высокая скорость передачи данных и возможность ее наращивания – ключевые характеристики сетевой инфраструктуры современного ЦОДа, которому приходится справляться со стремительно растущими объемами информации.

14,2 млрд – именно столько, по оценкам Gartner, различных устройств подключено к сети по всему миру сегодня. В 2021 г. их количество, по прогнозам, может достичь уже 25 млрд.

Поскольку количество подключенных устройств постоянно растет, по сетям передаются все большие объемы данных. По мере развития ИТ нагрузка на дата-центры увеличивается. Фактически ЦОДы находятся на переднем крае цифровой трансформации. Обработка постоянно растущих объемов сложных данных из множества источников требует, чтобы полоса пропускания становилась шире, а скорость передачи – выше.

Владельцам и операторам ЦОДов важно оценить, способны ли имеющиеся сети и кабельная инфраструктура их объектов поддерживать будущие потребности. Какие факторы им нужно учитывать при выборе кабельных систем и коммутационного оборудования? На какой рост скоростей и производительности ориентироваться?

Неважно, предназначен ли ЦОД для облачных сервисов или услуг colocation, собственный это ЦОД заказчика или узел гибридной системы, в любом случае для эффективной обработки большого объема сложных данных нужна надежная инфраструктура с широкой полосой пропускания и малым временем отклика. Она должна иметь разветвленную систему подключений для различного активного оборудования, расположенного как на периферии сети, так и на магистралях, ведущих к ядру и сетевым хранилищам SAN. Кабельная инфраструктура ЦОДа должна одновременно обеспечивать максимальную управляемость объекта и его масштабируемость по мере роста объема обрабатываемых данных и требований к пропускной способности.

На периферии сети…

В современных ЦОДах на периферии сети, между коммутаторами и серверами, уже необходима скорость не менее 25 Гбит/с, а в перспективе 40 Гбит/с и выше. Если говорить о требованиях к кабельной среде передачи, то нужно ориентироваться на медные системы категории 8, а именно:

- системы класса I, основанные на продукции категории 8.1, в которой используется интерфейс RJ45;
- системы класса II, основанные на продукции категории 8.2, в которой используются не-RJ-интерфейсы;
- экранированные системы категории 8, основанные на компонентах категории 8.

Все перечисленные кабельные системы имеют потолок частот до 2 ГГц, что позволяет поддерживать приложения 25 и 40 Гбит/с. Системы обеспечивают максимальную длину канала 30 м и рассчитаны максимум на два коннектора в канале. Проектировщики ЦОДа должны уметь располагать стойки и шкафы таким образом, чтобы вписаться в указанную длину. Это необходимо для перехода к приложениям 25G/40GBASE-T.

Если в ЦОДе принят подход Top-of-Rack, предусматривающий установку коммутатора в верхней части каждого шкафа, потребуются высокоскоростные шнуры для прямого подключения активного оборудования. Такой подход имеет свои плюсы. Высокоскоростные шнуры прямого подключения соединяют сетевой коммутатор с активным оборудованием – серверами, устройствами СХД, расположенными в том же или в соседнем шкафу. Фактически используется конфигурация «точка – точка». Такие шнуры обладают высокой пропускной способностью и дают возможность передавать большие объемы данных. Их могут называть по-разному:

- шнуры прямого подключения (Direct Attach Copper Cables, DACC);
- активные оптические шнуры (Active Optical Cables, AOC);
- трансиверные сборки.

Они поддерживают скорости от 10 до 100 Гбит/с, что позволит ЦОДу работать эффек-

тивно тогда, когда вместо 10-гигабитного активного оборудования будет устанавливаться 25-гигабитное и даже более скоростное.

Делая выбор между различными типами высокоскоростных шнуров прямого подключения, сетевые специалисты должны принимать во внимание дополнительные факторы – например, ограничения по длине шнуров, характерные для продукции разных изготовителей. Как правило, прямое подключение используется, когда оборудование располагается близко друг к другу – в соседних шкафах в ряду. Шнуры должны выпускаться в вариантах длин с шагом 0,5 м, чтобы для каждого случая можно было подобрать подходящий – скажем, шнурами длиной 0,5 м или 1 м подключать к коммутатору серверы из средней части шкафа, а шнурами длиной 1,5 или 2 м – устройства, расположенные ближе к основанию шкафа.

Чтобы избежать мешанины шнуров во внутреннем пространстве шкафа, следует задействовать кабельные органайзеры, каналы коммутации и другие средства упорядочивания кабелей. Применение соответствующих аксессуаров и шнуров из кабеля уменьшенного сечения способствует более эффективному доступу охлаждающего воздуха в шкафы.

...и в ее центре

Магистральные сегменты требуют принципиально иного подхода. Основная среда передачи в магистралях – волоконная оптика, а скорости постепенно приближаются к 200 и 400 Гбит/с. В список оптических решений, поддерживаю-

Строим ЦОД блоками

Потребности в вычислительных мощностях растут быстро, а в объеме систем хранения – еще быстрее, буквально с каждым часом. Тем, кто управляет ЦОДами, необходимо оперативно расширять емкость и улучшать характеристики объектов. Концепция модульных ЦОДов позволяет быстро и малыми усилиями организовать процесс расширения, не жертвуя надежностью и эффективностью работы объекта.

Модульная концепция опирается на понятие «точки доставки» (Point of Delivery, PoD) – своего рода строительного блока, модуля, обладающего определенной вычислительной мощностью и объемом СХД, укомплектованного сопутствующими компонентами и наборами приложений, которые вместе обеспечивают предоставление ИТ-услуг. Аппаратные шкафы в таком модуле чаще всего выстроены симметрично двумя рядами и образуют структуру горячих/холодных коридоров. Подобные группы шкафов обычно проектируются с учетом необходимой вместимости, функционального назначения и особенностей используемых приложений. С коммутаторами в ядре сети такие группы связаны, как правило, через коммутаторы уровня агрегации. Эти коммутаторы могут располагаться как внутри модуля, так и вне его – в отдельной зоне распределения, которая может обслуживать несколько модулей.

Если нужно расширить модульный ЦОД, к нему просто добавляются такие же «строительные блоки», что уже развернуты на объекте. Фактически первый модуль, установленный в самом начале, впоследствии служит шаблоном для создания и пристраивания новых блоков. Поскольку модули в ЦОДе представляют собой отдельные, самодостаточные отсеки, их можно просто добавлять в нужном количестве по мере роста потребностей. При таком подходе ЦОДы можно масштабировать быстро и с минимальными усилиями.

Для успешной реализации модульного подхода предусмотрена возможность заказывать шкафы в сборе, предварительно собранные поставщиком в соответствии с той или иной типовой конфигурацией. Шкафы поставляются с уже установленным медным и волоконно-оптическим коммутационным оборудованием. Их комплектуют блоками розеток для распределения питания (PDU), кабельными органайзерами и прочими необходимыми аксессуарами. Все компоненты уже предварительно собраны, комплект поступает в единой упаковке, и на объекте остается только распаковать шкафы, установить в них активное оборудование и выполнить финальные подключения. Как только заказчик определит типы конфигураций, которые ему нужны (шкаф для сетевого хранилища, сетевой шкаф, серверный шкаф), соответствующие компоненты включаются в спецификацию со всеми артикулами и необходимыми описаниями, и таким образом формируется ведомость материалов для каждого модуля в ЦОДе. Поскольку расширение объекта будет происходить по той же самой модульной схеме, владельцы и операторы ЦОДа могут заранее оценить будущие затраты на расширение и выделить ресурсы для таких работ.

Новые спецификации IEEE для протоколов физического уровня ▶

Приложение	Число волокон	Среда передачи (волокно)	Максимальное расстояние, км
200G-BASE-DR4	8	Одномодовое	0,5
200GBASE-FR4	2	Одномодовое	2
200GBASE-LR4	2	Одномодовое	10
200GBASE-SR4	8	Многомодовое	0,1 (OM4)
400GBASE-DR4	8	Одномодовое	0,5
400GBASE-FR8	2	Одномодовое	2
400GBASE-LR8	2	Одномодовое	10
400GBASE-SR16	32	Многомодовое	0,1 (OM4)

щих 200G и 400G, входят приложения 200GBASE-DR4, 200GBASE-LR4 и 400GBASE-DR4 для одномодовых сред и 400GBASE-SR16 для многомодовых. При этом реализация высокоскоростных приложений зависит от того, были ли изначально на объекте установлены подходящие оптические кабели. Какими же они должны быть?

Из данных таблицы следует, что и многомодовые, и одномодовые приложения (причем как 200-, так и 400-гигабитные) можно реализовать в оптических сегментах с количеством волокон, кратным двум или восьми. Так, одобренные стандартами IEEE приложения 200 и 400 Гбит/с для средних расстояний, до 500 м (что покрывает все типовые потребности ЦОДа и позволяет применять относительно недорогое оптическое активное оборудование), скорее всего, будут ориентироваться на восьмиволоконную конфигурацию BASE-8.

На сегодняшний день во многих ЦОДах установлены 12-волоконные сегменты MTP. Однако 12-волоконная конфигурация MTP не дает максимальной эффективности, ведь из 12 волокон только восемь реально задействованы в передаче сигналов. Если четыре волокна из 12 простаивают, не используется 33% ресурсов системы, а значит, треть системы была установлена напрасно.

Если же в ЦОДе проложить восьмиволоконные магистрали MTP, а для коммутации использовать восьмиволоконные шнуры MTP, то будут задействованы все 100% ресурсов кабельной системы. Восьмиволоконные решения MTP не только более эффективны и экономичны, обеспечивают поддержку 40- и 100-гигабитных приложений 40/100GBASE-SR4, но и рассчитаны на переход к приложениям следующих поколений – 200 и 400 Гбит/с.

Если в ЦОДах уже установлены 12-волоконные сегменты MTP, можно прибегнуть к специальным переходным (гибридным) шнурам и соединительным модулям, чтобы восьмиволоконные существующие и будущие приложения задействовали все имеющиеся в системе волокна: по двум 12-волоконным сегментам MTP с их помощью можно пропустить три восьмиволоконных приложения. В этом случае степень использования инфраструктуры составит 100%, но надо честно признать, что это более сложный и менее удобный путь, чем сразу закладывать в систему восьмиволоконные сегменты MTP. Ведь если в сети потребуется производить какие-либо работы или менять поврежденный шнур, то из эксплуатации придется вывести сразу три порта. Также нужно учитывать, что гибридные модули вносят дополнительные оптические потери в канал, и это может негативно сказаться на производительности системы.

Вносимые потери в высокоскоростных оптических сетях часто становятся предметом озабоченности и обсуждений. Совокупное затухание определяется потерями, которые вносят сама среда кабеля и соединения в канале. Чем выше скорость передачи в сети, тем строже требования к вносимым потерям, жестче пределы допустимых значений. К сожалению, принятые сейчас варианты архитектуры сетей – плоские, неиерархические, с малым количеством уровней коммутации – характеризуются большими расстояниями между коммутаторами, и это осложняет прокладку таких сегментов и последующее управление ими. Если предусмотреть между коммутаторами точки распределения или кросс-соединения, можно уменьшить протяженность кабельных сегментов и улучшить управляемость, но каждая точка распределения добавляет новые соединения, а значит, увеличивает оптические потери в канале. Выход только в том, чтобы для таких межкоммутаторных сегментов использовать продукцию серии MTP Low Loss – специально разработанные компоненты с уменьшенными оптическими потерями.

Поскольку объем данных, генерируемых устройствами IoT, растет взрывными темпами, владельцам и операторам ЦОДов необходимо проверить, сможет ли их сетевая инфраструктура удовлетворять постоянно растущие потребности в вычислительной мощности, скорости передачи и объеме сетевых хранилищ. Кабельную среду нужно выбирать таким образом, чтобы и сегменты на периферии сети, и магистрали в центре могли поддерживать самые продвинутые и требовательные приложения. В проекте ЦОДа обязательно должна быть предусмотрена возможность масштабирования. Только тогда центр обработки данных сможет соответствовать будущим вызовам. ИКС

ЦОД за шесть месяцев

Карантинные меры усложнили работы, но не помешали компании «Инфосистемы Джет» в кратчайшие сроки запустить контейнерный ЦОД для агрохолдинга «Русагро» в Уссурийске.

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

Чтобы поддержать бизнес в Приморье, агрохолдинг «Русагро» решил построить в Уссурийске edge-ЦОД для обработки данных 12 своих предприятий в регионе. Перед компанией «Инфосистемы Джет» была поставлена задача реализовать проект в сжатые сроки (шесть месяцев вместе с проектированием, поставкой оборудования и сдачей в эксплуатацию).

Изначально «Русагро» предполагал развернуть ЦОД в административном корпусе, но в этом случае к созданию дата-центра можно было приступить только после завершения его строительства. Для ускорения ввода в эксплуатацию наши специалисты предложили вынести ЦОД в отдельный контейнер.

Решение оказалось наиболее подходящим для задач агрохолдинга. Кроме того, использование опыта, накопленного компанией «Инфосистемы Джет» в создании контейнерных дата-центров (КЦОД), позволяло значительно ускорить реализацию проекта.

О логистике и тестах на коронавирус

Контейнер собрали на производстве в Екатеринбурге, где протестировали инженерную инфраструктуру. Испытания при полной тепловой нагрузке проводились в течение 72 ч по 372 пунктам методики. Затем контейнер частично разобрали и за две недели перевезли в Уссурийск.

Перевозку осложняли карантинные меры, различающиеся от региона к региону. Также специфику внесло дополнительное тестирование на коронавирус специалистов по инженерным системам, вычислительным комплексам и сетевому оборудованию. Только после того, как результаты были получены, мы приступили к работе.

На месте КЦОД был установлен на заранее подготовленную бетонную площадку и заново протестирован. Помимо инженерной инфраструктуры, рассчитанной на 11 стоек, мы поставили полный комплекс вычислительного оборудования и развернули сеть передачи данных. Все работы мы выполнили быстро и всего за пять дней ввели КЦОД в эксплуатацию.

Технические детали

Контейнер нестандартный, имеет ширину 3,15 м, что значительно облегчает обслуживание серверного оборудования. КЦОД может работать в любых погодных условиях и выдерживать диапазон температур от –40 до +40°С. Для зимнего периода предусмотрен подогрев воздуха в системе вентиляции. Использованы пароувлажнители замкнутого типа, не требующие подведения к водопроводу. Охлаждение также замкнутое, на фреоновых межрядных кондиционерах без фрикулинга, который не нужен при таких объемах. Интересное решение – быстросъемные силовые разъемы (розетки, с помощью которых подключается КЦОД). Таким образом, при необходимости его можно отключить от сети и перевезти на другое место.

Специально для этого проекта мы разработали систему мониторинга, контролирующую влажность и температуру в каждом шкафу, состояние дверей, параметры электрической сети, состояние автоматических выключателей, ИБП, ДГУ, систем пожаротушения, кондиционирования и вентиляции. Оперативное оповещение персонала осуществляется по локальной сети, электронной почте и с помощью SMS.

Контейнер установлен под открытым небом, поэтому имеет многослойное антикоррозийное покрытие с защитой от газа, огня, воды и пыли. Дверь – с двойным контуром подогрева, исключающим примерзание.

В системе противопожарной безопасности используется наиболее безопасный для человека газ Novec 1230. Защищаются не только зал со стойками, но и дополнительные технологические отсеки. Сигнал о пожаре поступает в систему пожарной сигнализации и службу безопасности всего объекта.

Решить задачу с помощью контейнера

Проект продемонстрировал преимущества контейнерных ЦОДов – возможность вести одновременно строительство здания, тестирование инженерных конструкций на заводе-изготовителе, где проще учесть все замечания заказчика, и транспортировку. Вынеся ЦОД из здания, мы не только ускорили работу, но и освободили 42 кв. м под офис.

ЦОД «Русагро» в Уссурийске с июня работает в режиме промышленной эксплуатации. Теперь к нашему опыту проектирования, развертывания и сопровождения контейнерных ЦОДов, транспортировки контейнеров авто- и железнодорожным транспортом добавился еще и удачный опыт работы в условиях карантинных ограничений.

Написать автору статьи

OCP – для ЦОДов больших и малых

Применение технологии OCP принесет максимальную выгоду операторам крупных дата-центров, но решения актуальны и для средних и небольших ЦОДов: среднегодовое значение PUE может снизиться до 1,1–1,15. Эффективным дата-центрам дорога открыта, остается по ней пойти.

Михаил Крупин, торговый представитель Bel Fuse в России

В 2011 г. Facebook запустила инициативу Open Compute Project (OCP), цель которой – подвигнуть разработчиков создавать универсальные продукты, делая ЦОДы более гибкими, легко масштабируемыми и простыми в эксплуатации, за счет чего снизить их CAPEX и OPEX. Впоследствии к сообществу OCP примкнули многие операторы и производители, благодаря чему применение решений OCP компаниями разного размера стало доступным и коммерчески целесообразным.

За 2019 г. рынок решений OCP вырос на 40%. Ожидается, что, несмотря на тяжелый 2020-й, в ближайшие три года этот рынок будет увеличиваться на 36% в год и к 2023 г. вырастет втрое. Такой прогресс обусловлен, в частности, расширением области применения технологий OCP – от ИТ-гигантов до предприятий банковской и транспортной сфер, ТЭК, операторов связи и правительственных учреждений.

В Россию новые технологии традиционно приходят с запозданием, но так же находят своих потребителей, и если ЦОДы, построенные на базе OCP, сейчас можно пересчитать по пальцам одной руки, то заинтересованных компаний – которые эксплуатируют или планируют запустить тестовые сайты – десятки.

КПД – всему голова

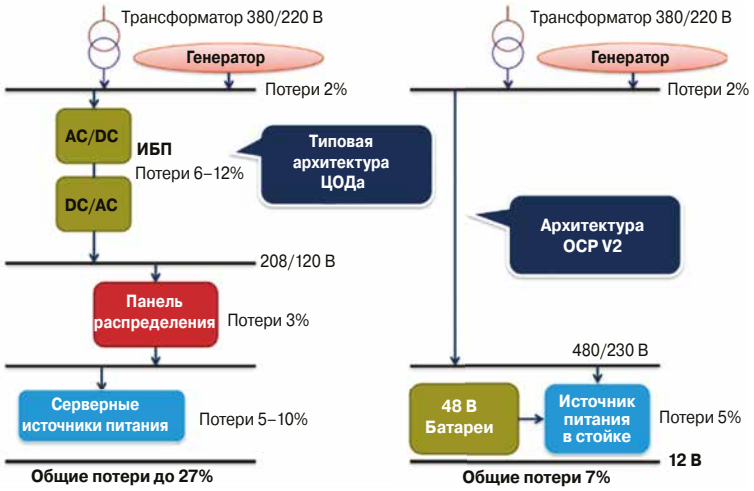
Еще в первом поколении своего OCP-оборудования Facebook перестала использовать резервные источники питания в серверных узлах, что позднее привело к полному отказу от встроенных преобразователей и выносу их в отдельный блок (так называемую силовую полку) в составе стойки.

Идея проста: встроенный в оборудование источник питания почти всегда преобразует переменное напряжение 220 В в постоянное 12 В, которое в дальнейшем понижается до напряжения потребителей внутри устройства (память, процессоры, диски и т.д.). Теперь же все оборудование в стойке питается напрямую от 12-вольтовой шины V2 (или трех шин V1), проходящей вдоль всей стойки, а силовая полка, чей выход подключен напрямую к шине, получает энергию от трехфазных вводов (чаще всего от двух независимых).

Первоначально полезная нагрузка одной стойки составляла 13 кВт, но впоследствии были реализованы проекты с мощностями, порой в разы превосходящими исходную. В рамках OCP предлагалось применять стойки увеличенной ширины 21 дюйм, поэтому неудивительно, что в 2016 г. возникло ответвление Open19, ориентирующееся на оборудование привычного 19-дюймового формфактора.

Вынос электропитания освободил пространство в стойке для дополнительных вычислительных мощностей и снизил удельную стоимость вычислений. Помимо этого, OCP предлагает использовать источники питания с КПД уровня 80 PLUS Platinum или Titanium. Высокий КПД и допустимый режим работы при температуре не менее +35°C означают снижение выделения тепла и потребляемой энергии, показателя PUE и соответственно расходов на охлаждение и на батарейный банк, повышение долговечности оборудования, сокращение занимаемых площадей, возможность применения фрикулинга в регионах, где это позволяют климатические условия. Все это положительно влияет на CAPEX. Отметим и многократное повышение скорости развертывания (по сравнению с решениями традиционных ЦОДов) за счет модульности оборудования и конструкции стоек, предназначенных для проведения вторичного монтажа исключительно с фронтальной стороны. Универсальность спецификаций делает решения OCP мультибрендовыми, а значит, обеспечивает потребителю выбор и конкурентные цены.

При передаче электроэнергии с главного ввода до ИТ-узла общий КПД снижается в основном на этапах



Потери электроэнергии в ЦОДе классической архитектуры и архитектуры OCP V2

коммутации. Любое преобразование напряжения ввиду применения трансформатора без потерь не обходится, а все потерянные ватты уходят в тепло. При традиционном подходе, оплатив, скажем, мощность 1 кВт, на выходе можно получить в среднем 750 Вт, а потерянные 250 Вт в виде тепла необходимо отводить с помощью систем охлаждения, увеличивая общую потребляемую мощность сверх упомянутого 1 кВт.

Для того чтобы избавиться от большей части коммутаций и еще сильнее повысить КПД, в последней версии архитектуры Open Compute Rack ИБП был перенесен из внешнего узла внутрь стойки. За счет этого среднегодовое значение PUE снизилось до значений 1,1–1,15 (в сравнении с 1,5 для среднестатистического традиционного ЦОДа). Для расположенного в Москве ЦОДа мощностью 1 МВт это означает экономию на электроэнергии до нескольких миллионов рублей в год. Благодаря подобным инновациям сама Facebook сэкономила $2 млрд за первые три года эксплуатации новых ЦОДов.

Помимо экономии на электроэнергии OPEX уменьшается и благодаря лучшей организации обслуживания ЦОДов. Модульность и фронтальный доступ к оборудованию значительно снижают требования к оснащению, а также к навыкам и численности персонала: один сотрудник может обслуживать десятки тысяч узлов. Быстрота и простота проведения ремонта сокращают и время простоя оборудования. А пониженный самонагрев преобразователей энергии продлевает их срок жизни.

Поскольку вычислительная техника относительно быстро устаревает и после нескольких лет эксплуатации в передовых ЦОДах зачастую отправляется на вторичный рынок, немаловажно, что силовые полки могут при этом оставаться на своих местах и использоваться с более современным оборудованием, что снижает затраты на дальнейшую модернизацию дата-центра.

Силовая полка Open Rack and Power

Силовая полка – центральный узел питания в стойке. Она представляет собой каркас шириной 19 или 21 дюйм и высотой 1 OU (1 Open Unit = 48 мм) с секциями для размещения шести силовых модулей «горячей» замены с фронтальной стороны и блейд-разъемом (или тремя) для подключения к силовым шинам с тыльной стороны. В состав полки может быть включен сетевой контроллер (NAC), поддерживающий распространенные сетевые протоколы и веб-интерфейс для удаленного мониторинга и управления питанием. В полке имеется схема байпаса и разъемы для резервированного питания традиционного оборудования от сети 220 В, например, коммутатора Top of Rack.

В общем случае, когда силовые полки запитаны от сети переменного тока, каждый из шести блоков питания работает от отдельной фазы. Когда к полке подключены два независимых ввода, реализуется схема резервирования 2N: три преобразователя работают от одного ввода, три – от другого. В случае, когда независимые вводы подключены каждый к отдельной полке, реализуется схема резервирования N + 1. При этом все блоки равномерно распределяют нагрузку между собой.

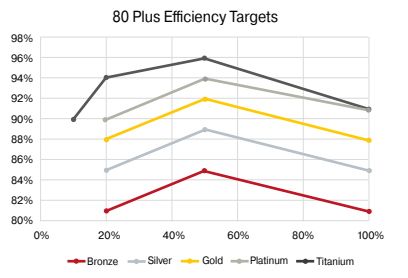
Типовые архитектуры питания

Типичная схема электропитания стойки OCP такова: от двух трехфазных вводов питаются силовые полки, которые вырабатывают 12 В и по силовым шинам (расположены на задней части шкафа) подают это напряжение на все оборудование в стойке. Типовые блоки питания представляют собой модули «горячей» замены мощностью 3,0 или 3,6 кВт с КПД уровня 80 PLUS Platinum или Titanium. Соответственно мощность одной полки достигает 15 или 18 кВт в постоянном режиме (с учетом схемы N + 1). Несколько силовых полок можно подключать параллельно, чтобы повысить уровень резервирования системы или нарастить мощность стойки. В сегменте высокопроизводительных вычислений востребована версия с шиной 48 В, поскольку дальнейшее наращивание мощности (при шине 12 В) привело бы к увеличению толщины проводника.

С ростом потребности операторов связи в системах виртуализации, грядущим внедрением 5G и необходимостью модернизации узлов связи, построенных на базе существующей инфраструктуры –48 В, востребованы и силовые полки с преобразованием напряжения –48 В в традиционные для OCP 12 В.

Таким образом, применение технологий OCP возможно не только при создании новых ЦОДов, но и при расширении действующих. Технология допускает использование различных электрических подключений, она гибка и проста в обслуживании, а стоявшая у истоков OCP компания Bel Power Solutions и ее опытные локальные эксперты окажут полную поддержку в проектировании, подключении и тестировании оборудования.

80 PLUS Platinum или Titanium?



▲ **КПД источников питания разных классов 80 PLUS**

Максимальный КПД обычно достигается при 50%-ной загрузке, но не менее важны его значения при пониженной и повышенной загрузке. Казалось бы, поскольку при 100%-ной загрузке КПД блоков Titanium и Platinum, согласно стандартам, не отличаются (блоки Bel Power класса Titanium имеют КПД на 1% выше Platinum при нагрузке 100%), покупка более дорогих Titanium нецелесообразна. Но это справедливо в основном для резервирования N + 1. При схеме 2N преобразователи Titanium позволяют увеличить КПД на 2–3% и, следовательно, экономят еще 2–3% электроэнергии. Когда речь идет о мегаваттах, это весомый аргумент.

Технологии индустриальной революции

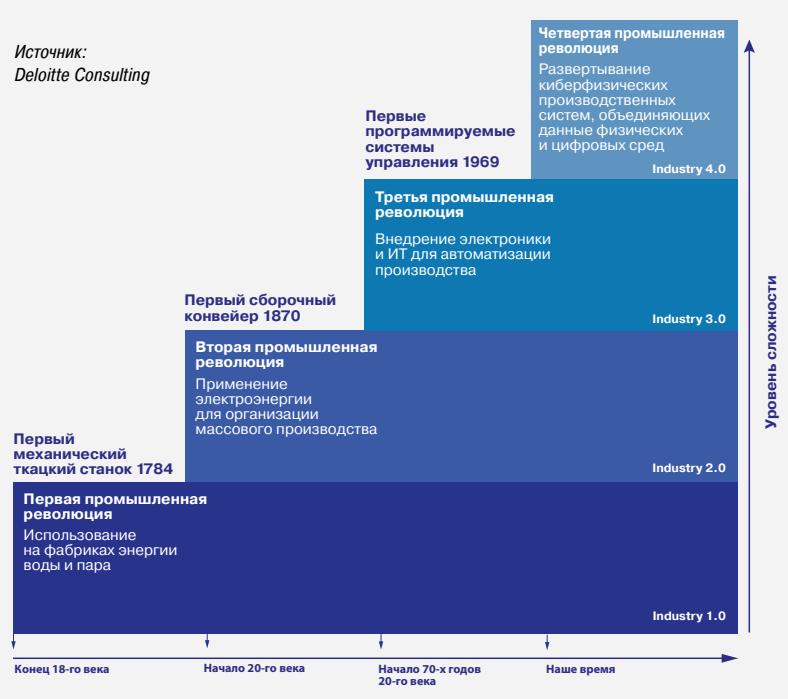
Алексей Черно-бровцев

Долгое время комплексы АСУ ТП и корпоративные ИТ-системы в промышленных организациях были мало связаны друг с другом. Четвертая промышленная революция коренным образом меняет ситуацию.

Новая парадигма использования современных информационных технологий и внедрение облачных решений являются эффективными инструментами повышения производительности предприятий различных областей экономики, включая промышленность. Цифровизации последней способствуют разработка концепций интернета вещей (IoT), промышленного интернета вещей (IIoT, он же промышленный интернет) и другие технологические достижения, стимулирующие развертывание процессов, которые в Европе называют четвертой промышленной революцией (Industry 4.0), а в Северной Америке – интеллектуальным производством (рис. 1).

Термин «Индустрия 4.0» предложили в 2011 г. в Академии инженерных наук при правительстве Германии для описания перехода от традиционной промышленной автоматизации к внедрению сетевых киберфизических систем в процессы производства и сбыта предприятий обрабатывающей промышленности.

Рис. 1. Характер промышленных революций ▼



Четвертая промышленная революция характеризируется конвергенцией операционных и информационных технологий производственных компаний. Фундаментом индустриальной цифровизации служит интернет вещей, предоставляющий недоступные ранее объемы данных и средства для их обработки и помогающий значительно повысить эффективность производственных и операционных процессов предприятий.

Промышленный интернет

IIoT позволяет создавать для автоматизации производственных предприятий индустриальные киберфизические системы, используя для этого достижения современных инфокоммуникационных технологий. Одна из основных идей промышленного интернета – минимизация влияния человеческого фактора на работу комплексов автоматизации предприятий.

Цифровизация на основе промышленного интернета открывает доступ к значительным объемам массивов производственных данных, поступающих из различных источников: установленных в цехах датчиков, АСУ ТП, хранилищ информации приложений управления, включая ERP (Enterprise Resource Planning), MES (Manufacturing Execution System), и ряда других систем. Их обработка ИТ-ресурсами, предоставляемыми комплексами IIoT, дает возможность формировать технологические и принимать управленческие решения, которые способны заметно повысить продуктивность промышленных компаний.

Анализ больших данных в промышленности и практическое использование его результатов являются наиболее существенными дополнениями к традиционным решениям автоматизации на базе программных диспетчерских систем SCADA (Supervisory Control And Data Acquisition), программируемых логических контроллеров (ПЛК), автоматизированных рабочих мест (АРМ) операторов и промышленных роботов.

Аналитики Boston Consulting Group рассматривают большие данные и методы их анализа

в качестве важнейших технологий индустриальной трансформации, к которым они относят также промышленный интернет, решения на базе автономных роботов, моделирование, горизонтальную и вертикальную интеграцию, кибербезопасность, дополненную реальность и аддитивное производство (рис. 2). Последнее использует цифровые модели и системы генеративного дизайна, позволяющие передавать ИТ-платформам часть функций проектирования. В Deloitte добавляют к этому искусственный интеллект, машинное обучение и когнитивные системы.

Новыми источниками производственной информации служат цифровые копии физических объектов и процессов, которые применяются в приложениях моделирования, группы совместно работающих роботов, а также роботы, помогающие в работе персоналу предприятий.

Промышленный интернет не ограничивается простым подключением устройств, сбором, хранением и анализом данных. IIoT открывает пути к модернизации технологий и оптимизации экономики производственных процессов, обеспечивает взаимодействие с распределенными сетевыми структурами управления современных интеллектуальных производственных систем и, что не менее важно, ранее установленных устройств и машин, позволяя применять в современных технологических средах многочисленные решения, разработанные за последние десятилетия создателями систем автоматизации производственных процессов. Более того, IIoT разрушает барьеры, традиционно разделяющие команды специалистов подразделений информационных и операционных технологий промышленных компаний.

▲ **Рис. 2. Технологии, преобразующие промышленное производство**

Индустриальные облака и платформы

Основной парадигмой четвертой промышленной революции становится облачное производство, объединяющее существующие индустриальные модели автоматизации и корпоративные информационные технологии и охватывающее полный жизненный цикл продуктов – от проектирования, моделирования, изготовления и тестирования до эксплуатации и технического обслуживания.

Производства нового типа поддерживаются промышленными платформами IoT и распределенными системами индустриальных облаков (Industrial Clouds), которые содержат пулы взаимосвязанных виртуализированных ИТ-ресурсов, средства интеллектуального управления ими, предоставляют по запросам услуги различным категориям специалистов, вовлеченным в производственный цикл. Индустриальные облака позволяют оплачивать только потребляемые пользователями ИТ-ресурсы (модель pay as you go) в рамках хоро-

Источники: 451 Research, Forrester, Gartner

шо известных на корпоративном рынке сервисных моделей.

Сервис «инфраструктура как услуга» (IaaS) обеспечивает доступ к информационно-технологическим ресурсам; «программное обеспечение как услуга» (SaaS) позволяет применять готовое прикладное ПО, полностью обслуживаемое провайдером; «платформа как услуга» (PaaS) дает возможность пользоваться средами разработки и развертывания облачных приложений, операционными системами, СУБД, связующим ПО, средствами тестирования и другими размещенными у провайдеров инструментами.

Поставщики индустриальных облачных услуг стараются обеспечить их соответствие рекомендациям ассоциации Open Connectivity Foundation, которая занимается стандартизацией экосистемы интернета вещей и унификацией IoT-стандартов, гарантирующих безопасность подключений и устройств в различных облачных средах.

Многие облачные провайдеры, включая Amazon, Google, Microsoft и IBM, дополняют свои предложения сервисами поддержки интернета вещей. Игроками этого рынка становятся также ведущие операторы связи, обладающие развитой коммуникационной инфраструктурой. Эффективными инструментами для реализации современных решений IIoT служат облачные платформы и услуги, предоставляемые Amazon Web Services (AWS) и Microsoft Azure.

Корпорация Microsoft десятилетиями занимала лидирующие позиции в области ПО для промышленной автоматизации. С 1990-х гг. она поставляла инструменты и решения поддержки операционных технологий (OT), включая ОС и СУБД SQL Server, широко распространенные в том числе в MES-системах управления производством. Многолетний опыт сотрудничества Microsoft с разработчиками OT-решений оказал заметное влияние на выбор последними облачных сервисов корпорации для развертывания платформ IIoT.

В течение последних лет заметно укрепились позиции облачных сервисов AWS в промышленности. На их основе разрабатываются SaaS-комплексы для производственных компаний, развивается экосистема разработчиков и пользователей, в состав которой входят такие индустриальные гиганты, как Georgia-Pacific, Siemens и Volkswagen, заинтересованные в переходе к моделям Industry 4.0.

Наряду с промышленными облаками общего назначения существуют специализированные облачные решения Industry Clouds, предназначенные для различных вертикальных рынков. Такие отраслевые облака, учитывающие специфику определенных рыночных секторов, обеспечивают соответствие принятым в них деловым, операционным, юридическим и другим нормам, включая требования безопасности.

Рынок сегодня заполнен множеством платформ IIoT, создатели которых предлагают их промышленности, коммунальным и управляющим компаниям, другим подобным организациям в качестве инструмента перехода к технологиям Industry 4.0.

Сбор данных в комплексах Industry 4.0

Один из важнейших компонентов промышленного интернета – инфраструктура сбора данных датчиков АСУ ТП. Для ее создания на рынке имеются несколько десятков предложений с применением традиционных и беспроводных протоколов и технологий.

К проводным решениям относится однопарная сеть Ethernet, к работе над которой институт IEEE приступил в начале 2017 г. Стандарт IEEE 802.3cg Single Pair Ethernet регламентирует формирование «коротких» двухточечных и многоточечных 25-метровых сетей, а также «длинных» двухточечных соединений с расстоянием между узлами до 1000 м. Для таких сетей разработаны две модификации технологии физического уровня – 10Base-T1S и 10Base-T1L, которые определяют передачу данных по одной сбалансированной витой паре с быстродействием 10 Мбит/с.

Сети IEEE 802.3cg предоставляют возможность передавать данные по кабелям связи с одновременной подачей напряжения электропитания по технологии Power over Data Line. Они совместимы с существующими стандартами Ethernet, включая форматы и размеры пакетов.

Установка в датчиках, камерах и других устройствах интерфейсов IEEE 802.3cg Single Pair Ethernet унифицирует кабельную инфраструктуру Industry 4.0 и упрощает ее, поскольку в сетях Fast Ethernet (100 Мбит/с) для передачи данных требуется две, а в Gigabit Ethernet – четыре пары проводов.

Спецификация 802.3cg-2019 – IEEE Standard for Ethernet – Amendment 5: Physical Layer Specifications and Management Parameters for 10 Mb/s Operation and Associated Power Delivery over a Single Balanced Pair of Conductor – утверждена в 2020 г. Опубликован также международный стандарт IEC 63171-6 для соединений однопарного Ethernet в промышленных приложениях.

Для организации беспроводных коммуникаций в комплексах IIoT предлагаются энергоэффективные персональные сети малого радиуса действия Low Power Short Range Networks, большого радиуса – Low Power Wide Area Networks (LPWAN), а также решения на основе сотовых сетей.

В сетях малого радиуса физический уровень и управление доступом регламентируются стандартом IEEE 802.15.4, который служит основой для таких протоколов, как Zigbee, WirelessHART, MiWi, ISA100.11, Thread. Zigbee, к примеру,

В Gartner отмечают обилие схожих по возможностям IIoT-платформ. В выпущенном в июне 2019 г. отчете Magic Quadrant for Industrial IoT Platforms лидеры этого сегмента рынка ПО и стремящиеся занять такие позиции компании-претенденты не указаны. Тем не менее ведущие аналитики относят к наиболее перспективным платформенным продуктам Atos Codex IoT, Hitachi Lumada, IBM Watson IoT Platform, Microsoft Azure IoT, Oracle IoT Cloud, PTC ThingWorx, SAP Leonardo IoT, Schneider Electric EcoStruxure, Siemens MindSphere, Software AG Cumulocity IoT. При выборе учитывались такие факторы, как опыт работы вендоров платформ IIoT в области индустриального ПО, применимость предлагаемых решений для широкого спектра сценариев, известность и размер организаций-разработчиков.

Тенденции рынка

Трансформация производства на основе технологий Industry 4.0 становится реальностью. Основные направления преобразований промышленных компаний продемонстрировали, в частности, экспоненты выставки Hannover Messe 2019. Одна из важнейших тенденций – освоение крупнейшими автостроительными компаниями облачных решений гиперскейлеров. В BMW это делают вместе с Microsoft, в Volkswagen – с AWS и Siemens MindSphere.

Индустриальное облако Volkswagen Industrial Cloud, находящееся на завершающей стадии разработки, станет не только промышленной корпоративной, но и партнерской сетью. Решения и приложения Volkswagen будут доступны в рамках открытой экосистемы компаниям-партнерам. В 2020 г. сеть должна охватить около двух десятков производственных площадок Volkswagen Group. Консолидированная аналитическая обработка данных всех 124 заводов группы и сетевое взаимодействие с 1500 поставщиками приведут, как ожидается, к экономии средств в несколько миллиардов евро. Вклад в эту сумму от ввода в действие первых полутора десятков приложений, стандартизированных для всех заводов, должен составить около 200 млн евро. Предполагается, что развертывание Volkswagen Industrial Cloud позволит к 2025 г. увеличить производительность группы компаний на 30%.

Разработчики промышленного ПО предлагают инструменты оркестровки для развертывания мультивендорных комплексных решений, которые исключают привязку заказчиков к продуктам только конкретных вендоров. Такие решения охватывают в том числе процессы управления эффективностью производственных активов, включая управление жизненным циклом продуктов, ориентированное на безотказность технического обслуживания на основе условий, и прогнозную аналитику.

В этой области весьма активны AspenTech, GE Digital, Uptake, IBM и SAP, а также ряд других компаний. Значительные средства в IoT-приложения, ориентированные на рост производительности промышленности, эффективно-

подходит для приложений IoT среднего радиуса действия с равномерным распределением узлов на расстояниях до 100 м. Эта технология применяется обычно в ячеистых топологиях для расширения зоны покрытия путем ретрансляции данных датчиков через несколько узлов. Используется, как правило, в системах интеллектуального освещения, безопасности, управления энергопотреблением.

Сети LPWAN, в свою очередь, применяются в крупномасштабных комплексах IoT, охватывающих промышленные и коммерческие кампусы. Они предназначены для передачи небольших объемов данных из многочисленных конечных точек через довольно длительные промежутки времени.

LPWAN характеризуются низким энергопотреблением и минимальной мощностью передаваемых сигналов, обеспечивают связь на расстояниях не менее 500 м от шлюзов до конечных точек. LPWAN поддерживаются такими стандартами и технологиями, как SigFox, Symphony Link, Nwave, Ingenu (RPMA), Weightless, LoRa.

На наиболее ресурсоемкие приложения с интенсивными коммуникациями рассчитаны сети пятого поколения с быстродействием более 20 Гбит/с. Однако, что наиболее важно для IIoT, сети 5G позволяют подключать более 1 млн устройств, размещенных на площади 1 кв. км, и обеспечивают задержку передачи сигналов, не превышающую единиц миллисекунд.

Первая в России промышленная сеть пятого поколения введена в действие в 2020 г. на заводе КАМАЗ в Набережных Челнах. Она поддерживает технологии 5G и LTE и на первом этапе используется для видеонаблюдения, групповой связи, защищенного доступа к локальным информационным ресурсам, а также для VR/AR-решений и удаленного обучения персонала. Во время тестирования, по данным разработчиков, максимальное быстродействие в стандарте LTE достигло 46 Мбит/с, а в стандарте 5G – 870 Мбит/с. Использование диапазона LTE 2100 МГц для передачи сигнальной информации сети пятого поколения позволило существенно увеличить зону покрытия базовой станции 5G в диапазоне 28 ГГц.

Такие частные беспроводные сети связи для ведомственных приложений являются, как правило, коммуникационными решениями для взаимодействия устройств в рамках одного предприятия. Стандартизация технологий и решений 5G, как ожидают, завершится к 2021 г. Одной из главных проблем остается выбор частотных диапазонов.

сти использования производственных активов, управления людскими ресурсами и парками транспортных средств, инвестируют и в Oracle. Формируются также партнерские экосистемы для создания цифровых двойников. Примеры такого сотрудничества демонстрируют Siemens и Bentley Systems, PTC и Rockwell, ABB и Dassault Systems, Schneider Electric и Aveva.

Архитектурные различия

Важнейшая архитектурная особенность современных комплексов автоматизации – применение технологий кибербезопасности для ИТ-поддержки операционных процессов промышленных предприятий, включая глубокую защиту информации, автоматическое обнаружение аномалий и угроз, анализ трафика, мониторинг поведения оборудования, шифрование соединений и другие технологии борьбы с современными киберугрозами.

Обеспечить безопасность комплексов на базе промышленного интернета призваны в том числе рекомендации Industrial Internet Security Framework, выпущенные глобальным некоммерческим партнерством Industrial Internet Consortium, выявляющим, тестирующим и продвигающим лучшие практики в области IIoT.

Повысить защищенность производственных систем способны и сами индустриальные облака, поскольку методы и технологии киберзащиты, которые предлагают провайдеры облачных услуг, зачастую гораздо эффективнее локальных решений производственных компаний. Провайдеры следят за постоянными обновлениями информационной защиты, внедряют новейшие системы управления событиями и информационной безопасностью (Security Information and Event Management, SIEM), осуществляют резервное копирование и упрощают процедуры восстановления в случае потери данных из-за возникновения нештатных ситуаций.

Промышленный интернет оказывает также влияние на изменение традиционных комплексов АСУ ТП. В Honeywell Process Solutions, к примеру, предлагают на основе IIoT переход от традиционных (датчики – ПЛК – АРМ) к двухуровневым решениям, состоящим из защищенных облачных платформ и связанных с ними сетевой инфраструктурой периферийных комплексов. Такие периферийные комплексы являются гетерогенными средами, в состав которых входят датчики, исполнительные устройства, контроллеры и средства взаимодействия с операторами.

Периферийные вычисления и поддерживающие их системы становятся важнейшими связующими звеньями, осуществляющими взаимодействие АСУ ТП, комплексов управления и индустриальных облачных сред. Дело в том, что оперативные производственные процедуры тесно связаны с технологической инфраструктурой предприятий, срок службы которой измеряется десятилетиями, а программно-аппаратные решения граничных комплексов позволяют поэтапно с минимальным нарушением существующих операций внедрять новые технологии, постепенно модернизировать ПО и приобретать ИТ-услуги.

К очевидным преимуществам граничных сред относятся предварительная обработка исходных данных в непосредственной близости от их источников, сокращающая время формирования управляющих воздействий и существенно снижающая нагрузку на локальные и глобальные сети. Периферийные вычисления обеспечивают быстрый отклик для принятия решений в режиме реального времени.

Граничные решения различаются по степени сложности в зависимости от выполняемых функций. Это могут быть и IIoT-шлюзы, поддерживающие стандартные промышленные протоколы и способные взаимодействовать с облачными ресурсами и устройствами визуализации АСУ ТП, и ЦОДы «в коробках», содержащие локальные озера данных, системы искусственного интеллекта и машинного обучения, и фрагменты полноценных дата-центров. Инфраструктурные компоненты для них предлагают многие производители аппаратуры и ПО – от разработчиков устройств АСУ ТП до грандов инженерной инфраструктуры и известных ИТ-вендоров.

Так, в Hewlett Packard Enterprise разработали открытую платформу HPE Edgeline OT Link Platform, которая на границе сети автоматизирует взаимодействие OT-систем и ИТ-приложений управления данными. Платформа, утверждают в HPE, формирует экосистему работающих в периферийных и облачных средах сторонних приложений. В нее входят решения AWS, Google, Microsoft, SAP, PTC, GE и других компаний, предоставляющие информацию всем подразделениям предприятий и участникам цепочек поставок.

Среди решений Dell Technologies – промышленные шлюзы Edge Gateways серий 3000 и 5000, поддерживающие такие стандарты и протоколы, как Bluetooth Low Energy, Zigbee, GPS и CANopen.

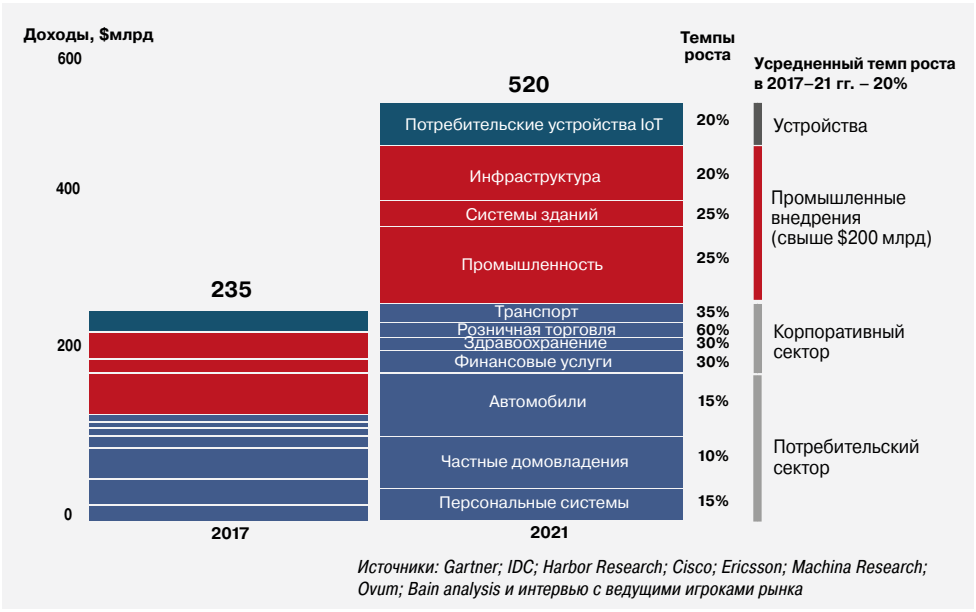
Концерн Schneider Electric поставляет в том числе изготовленные и протестированные на заводах контейнерные решения для ЦОДов и комплексы Micro Data Center Xpress, корпуса NetShelter, литий-ионные ИБП, системы охлаждения.

Industry 4.0 и российские ИТ-компании

Industry 4.0 ставит задачи, с которыми хорошо знакомы специалисты ИТ-подразделений: выбор

облачных платформ и их поставщиков, развертывание облачных сред, как правило, гибридных, определение того, в каком соотношении внедрять сервисы IaaS, PaaS и SaaS. Решение этих задач открывает новые возможности для формирования партнерских связей производственных предприятий с сервисными ИТ-компаниями. В число последних входят и крупные системные интеграторы, которые имеют опыт разработки заказных программных решений, располагают дата-центрами и облачными платформами.

В 2019 г. около 40% российского рынка IoT пришлось на бизнес-услуги. Такие сведения опубликованы IDC в отчете «Возможности и тенденции интернета вещей: углубленный анализ российского рынка». Объем этого рынка достиг $3,7 млрд, увеличившись в 2019-м более чем на 8% по сравнению с предыдущим годом. На первое место вышли производственные компании, за ними следовали предприятия транспортной отрасли и консьюмерского сегмента. По прогнозам IDC, среднегодовой показатель роста рынка интернета вещей до конца 2023 г. приблизится в нашей стране к 20%. В то же время аналитики ожидают роста объема мирового рынка промышленного интернета до $200 млрд уже к 2021 г. (рис. 3).



Источники: Gartner; IDC; Harbor Research; Cisco; Ericsson; Machina Research; Ovum; Bain analysis и интервью с ведущими игроками рынка

▲ Рис. 3. Доходы от поставок решений IoT и средств аналитики по сегментам рынка и темпы их роста

Такие перспективы должны стимулировать разработку решений Industry 4.0 игроками ИТ-рынка. Российские системные интеграторы способны оказать здесь неоценимую помощь отечественным, в том числе региональным, компаниям различного масштаба, участвуя в модернизации существующих и внедрении новых комплексов автоматизации на базе IIoT. ИКС

Цифровизация. Знания. Партнерство

Роман Монахов

В рамках расширения партнерской программы компания C3 Solutions открыла учебный центр для дистанционного обучения специалистов рынка инженерного оборудования дата-центров.

Пандемия резко ускорила процессы цифровизации, удаленная работа стала повседневной практикой предприятий. Как в современных условиях организовать обучение специалистов? Что предлагает бизнес? На вопросы нашего издания отвечает директор по продажам и маркетингу C3 Solutions Роман Монахов.

– Роман, почему компания C3 Solutions решила создать центр обучения? Кто будет в нем заниматься? Когда центр начал работу и почему информации о нем нет в интернете?

– Компания часто сталкивалась с ситуацией, когда партнерам и пользователям нашего оборудования не хватало знаний о работе с инженерной инфраструктурой дата-центров. Цель создания центра обучения C3 Solutions – повышение компетенции партнеров, помощь в изучении инженерных решений для инфраструктуры ЦОДов на примере решений нашей компании.

У компании C3 Solutions есть партнерская программа, обеспечивающая максимально комфортные условия для работы интеграторов, дистрибьюторов, коммерческих дата-центров. Она включает авторизованных, серебряных, золотых и технологических партнеров. Созданный учебный центр – один из элементов партнерской программы. В интернете информацию о нем найти трудно, так как центр совсем новый, дата запуска – 1 июля, а начало учебного процесса – 1 августа. Но на рынке о центре знают, формируются учебные группы: у компании уже более 30 заявок от партнеров.

– Почему решили использовать дистанционный формат обучения?

– Цифровизация – залог успешного бизнеса. Общее направления развития компании C3 Solutions – перевод взаимодействия с партнерами в режим онлайн. Уже работает онлайн-конфигуратор для самостоятельного составления спецификации, получения 3D-модели собранного оборудования, а также конфигуратор цветов для микроЦОДов. Цель – полная автоматизация: партнер заходит на сайт, выбирает решение, размещает заказ, отслеживает статус и получает его без участия наших сотрудников. Дистанционный учебный центр – еще один шаг в этом направлении. Компания повышает уровень компетенций партнеров, не заставляя терять время на дорогу и физически посещать учебный класс.

Правильность выбора формата подтвердила работа в период пандемии и самоизоляции, когда многие предприятия вынужденно перешли на «удаленку». Да и не всем легко до нас добраться. Наш бизнес выходит за пределы Российской Федерации, компания C3 Solutions работает со странами Восточной Европы и Центральной Азии, в планах – страны Ближнего Востока. Дистанционное обучение поддержит партнеров не только в России, но и по всему миру, даст им возможность ознакомиться с решениями нашей компании.

Конечно, можно получить знания и в режиме офлайн в демозале в центре Москвы. Если есть желание – приезжайте и изучайте оборудование «живьем». Встретим, все покажем, даже в выходные. Но лучше обучаться в свободное время и в удобном месте. Компания хочет подстроиться под партнера, а не заставлять партнера подстраиваться под нее.

Не стоит заставлять человека из Владивостока или Хабаровска ехать в Москву, чтобы получить сертификат для работы с оборудованием. Вебинар назначается на определенное время, но, если у партнера нет возможности в этот момент подключиться, ему предоставляются презентация и запись. Тестирование слушатели проходят в любое время – результаты проверяются автоматически.

При доставке решения вместе с оборудованием приезжает инженер, который при необходимости доучит партнера на месте, объяснит оставшиеся непонятными после онлайн-курса тонкости.

– Сколько стоит обучение? Кто может записаться на курсы?

– Центр открыт для всех игроков рынка. Обучение бесплатное. У компании нет цели его коммерциализировать. Мы хотим нарастить уровень компетенции наших партнеров и конечных пользователей. Мы стремимся не только обучать инженеров, производящих оборудование, но и развивать партнеров и конечных пользователей, вовлекая их в совместные разработки, помогая им глубже разбираться в инфраструктурных решениях, предъявлять более высокие требования к оборудованию. Пройдя обучение, слушатели поймут, что российское оборудование не уступает решениям зарубежных производителей.

Учебный центр – наш вклад в развитие рынка инженерных инфраструктурных решений для дата-центров. Игроки нашего, прямо сказать, небольшого рынка должны помогать друг другу расти профессионально. Чтобы было не стыдно сравнивать нашу отрасль ЦОДов с отраслями других стран.

– Какие курсы предлагает ваша компания?

– В учебном центре три вида курсов. Первый, Sales training, – базовый курс по продуктовым линейкам для account-менеджеров. Включает основные характеристики оборудования, принципы работы с компанией C3 Solutions, методику продаж решений. Курс рассчитан на партнеров – системных интеграторов и дистрибьюторов.

Второй, Tech training, рассказывает о технологических аспектах, конструктивных особенностях стоек, блоков распределения питания, систем кондиционирования и другого оборудования инженерной инфраструктуры дата-центров. Обучение проводится на примере продукции нашей компании, но полученные знания могут быть успешно применены в работе с оборудованием других вендоров. Помимо партнеров тренинг рассчитан на конечных клиентов.

Третий курс, Experts training, предназначен для технических специалистов, обслуживающих решения, прежде всего инженеров, которые устанавливают и сопровождают инженерные решения C3 Solutions.

– Как проходит процесс обучения? Как проверяются полученные знания?

– Зарегистрировавшись на нашей платформе, слушатель получает доступ к информационным материалам, загруженным видеороликам, каталогам и учебным курсам.

Учащийся прослушивает вебинары в удобное для него время, изучает презентации, потом проходит тестирование. Курс состоит из нескольких блоков, соответствующих нашим решениям из продуктовой линейки. Для некоторых групп предусмотрены онлайн-вебинары, когда в реальном времени можно задать вопросы руководителю департамента R&D. Такие вебинары впоследствии также доступны в записи.

Для завершения обучения надо сдать тесты по всем блокам. После успешного прохождения курса пользователю выдается сертификат.

– Что дает выпускникам полученный сертификат? Сколько времени займет учеба?

– Партнеру для сохранения статуса нужно иметь соответствующее число сертифицированных специалистов. У золотого партнера должен быть инженер, прошедший все три курса, у серебряного – два курса, у авторизованного – один.

Интересен курс и для самого учащегося. Прошедший обучение слушатель получает максимальную компетенцию по инженерной инфраструктуре C3 Solutions, повышает свою стоимость на рынке труда.

Курс Sales training можно пройти достаточно быстро. Тестовая группа прошла его за неделю, занимаясь три дня по два часа.

– Какие курсы пользуются наибольшей популярностью? Кто преподает на курсах и каков уровень их экспертизы?

– Пока нельзя сказать, что какой-то курс менее интересен. Заявки поступают на все курсы.

Преподаватели – специалисты компании C3 Solutions с многолетним опытом работы в отрасли. В будущем планируется при необходимости привлекать экспертов рынка, имеющих опыт эксплуатации нашего оборудования. Возможно, такие эксперты появятся в нашем центре уже осенью.

– Как технически организован центр обучения? Какие используются аппаратные и программные средства? Как можно подключиться к центру?

– Компания C3 Solutions использует облачную обучающую платформу, которая включает конструктор курсов и тестов, решения для организации вебинаров, библиотеку готовых курсов, аналитику и поддержку мобильных приложений. В режиме конференции преподаватель и студенты видят друг друга и могут задавать вопросы. В режиме вебинара преподаватель читает лекцию, а студент обращается к администратору с просьбой передать вопрос. Все зависит от формата учебного процесса. Решение персонализировано под требования C3 Solutions.

– Каковы технические требования к удаленным рабочим местам студентов?

– Для обучения слушателям достаточно иметь выход в интернет, стационарный компьютер с веб-браузером, планшет или смартфон. Студентам не нужен защищенный канал с платформой – достаточно войти и зарегистрироваться на сайте.

– Компания вкладывает в обучающий центр деньги, отвлекает ресурсы, затрачивает рабочее время сотрудников. А что это дает C3 Solutions? Компания привязывает к себе пользователей?

– Это не основная цель. Прошедший обучение слушатель не обязан что-либо у нас покупать. Если пользователь в ходе обучения убедится, что наше оборудование отвечает самым высоким требованиям, и станет закупать больше – это замечательно. Но самое главное – компания получает лояльность рынка. Развиваясь сами, мы хотим помогать развиваться партнерам. Компания достигла такого уровня зрелости, когда неинтересно просто заработать. Мы хотим нарастить уровень компетенции рынка инженерного оборудования для ЦОДов в России, возродить инженерный потенциал страны. Считаем это крайне важной задачей.

Рынок IaaS: время строить бренды

Николай Носов

На смену разорившимся в период кризиса клиентам облачных провайдеров придут новые. Борьба за них уже началась. Выиграет тот, кто сохранит активность, не остановится в развитии сервисов и клиентской базы, продвижении и повышении ценности бренда.

Делать прогнозы дальнейшего развития облачного рынка в условиях пандемии и экономического кризиса – все равно что нащупывать путь к двери в темной комнате. С одной стороны, компании массово переводят сотрудников на удаленный режим работы и даже после смягчения карантинных мер не вернут всех обратно в офис. Это положительный фактор для облачных сервисов. С другой стороны, обусловленный пандемией экономический кризис неизбежно уменьшит клиентскую базу облачных провайдеров.

Более или менее уверенно чувствует себя крупный бизнес, не пострадают в ближайшей перспективе и клиенты из госсектора, а вот будущее среднего и малого бизнеса вызывает опасения. Скорее всего, во многих отраслях экономики пройдет волна банкротств. Оставшиеся увеличат использование облачных ресурсов, но выживут не все, и часть клиентов облачных провайдеров уйдет с рынка. Но им на смену неизбежно придут новые...

Понять клиента

...Все изменилось вмиг. Пандемия, карантин, самоизоляция. Выход из квартиры – как вояж сталкера в Зону. Прихожая – как шлюзовая ядерного реактора. Поход за покупками – стресс.

Магазин – минное поле. Справа подбирается мужчина без маски – надо все бросить и уйти влево. Слева приближается не думающая о социальной ответственности за безопасную дистанцию молодая женщина. Скорее что-нибудь схватить на вечер и, задерживая дыхание, к самому опасному объекту – кассе. И только безнал. И не забыть по возвращении домой протереть пластиковую карточку или смартфон дезинфицирующими салфетками.

Кошмар, который несколько месяцев назад маркетологу не мог и присниться. Анализ перемещения покупателя по магазину, оптимальное расположение товаров на полках – все нужно делать заново, старые исследования теряют актуальность. Нужны новые, которые позволят понять и предсказать поведение клиента в резко изменившихся условиях. Это справедливо и для облачного рынка, ведь облака стали таким же массовым товаром, как гречка.

Облако как хранилище

«Все говорят – “облако”, “облако”. А что это, не понимаю. Объясни на пальцах», – попросил старый знакомый, работающий в Москве депутатом. Пробую рассказать: «Видишь в электронной почте раздел “облако”? Переносишь туда файлы. Потом можешь войти в этот раздел с другого устройства и скачать их оттуда. Или даже открыть доступ мне, чтобы я мог их просмотреть».

Облака и сегодня на бытовом уровне воспринимаются большинством как некое удаленное файловое хранилище. Спасибо почтовым сервисам, которые показали преимущества новой технологии массовому пользователю и фактически ввели понятие «облако» в повседневный обиход.

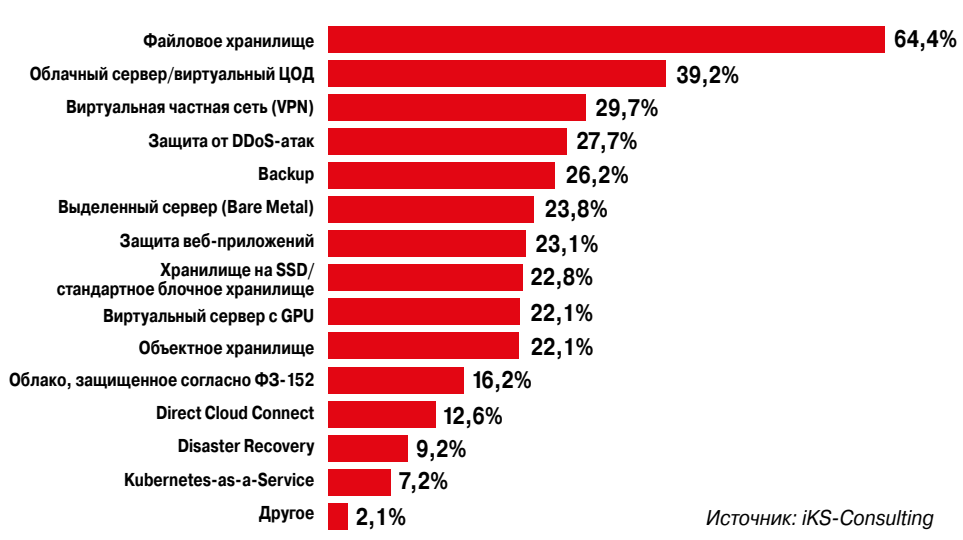
Популярность облачных услуг у российских предприятий продолжает расти. Это подтверждают последние исследования iKS-Consulting, проведенные в феврале-марте текущего года: из почти 400 респондентов 67% заявили, что за последние три месяца пользовались услугами или продуктами облачных провайдеров.

Опрос проводился до начала пандемии, так что сейчас процент пользователей облачных сервисов наверняка вырос. В нынешних условиях вводить в эксплуатацию новые аппаратные решения непросто, и многие потребители, вынужденные искать оперативное решение своих бизнес-задач, прибегают к аутсорсингу. Карантинные меры и кризисные явления в глобальной экономике стали драйверами развития аутсорсинга и повсеместно, невзирая на отрасли, ускорили процессы перехода на сервисную модель.

Что касается сервисов, то в бизнесе, как и у конечных пользователей, самой популярной облачной услугой, которую отметили 64,4% респондентов, опрошенных iKS-Consulting, остается файловое хранилище (рис. 1). Облака используют как круглосуточно доступный архив, как банк данных с разграничением доступа на скачивание.

Служат облака и для хранения резервных копий (к этой услуге обращались 26,2% респондентов). При организации резервного копирования часто ориентируются на правило «3-2-1»,

Рис. 1. Общая структура использования облачных услуг ▼



Источник: iKS-Consulting

Источник: iKS-Consulting

Рис. 2. ▶ Приоритизация критериев выбора облачного провайдера

которое гласит, что для надежного хранения нужны три копии, физически находящиеся в разных местах, на двух типах носителей, причем одна копия должна храниться вне офиса. Если компания пользуется облачными сервисами, то копии должны храниться на площадке клиента и в двух разных облаках.

Как правило, такие задачи не предъявляют высоких требований к времени задержки при передаче данных по каналам связи, что позволяет стать участником рынка этой услуги всем российским, а при соблюдении требований отечественного законодательства и зарубежным дата-центрам.

Виртуальный сервер

Прошли времена, когда на конференциях «ИКС-Медиа» из зала задавали вопросы типа: «Со скольких процессоров компьютер можно считать облаком?». Второе место по востребованности (39,2%) занимает классическая облачная услуга – облачный сервер (виртуальный ЦОД) (см. рис. 1). Эта услуга особенно популярна у крупного бизнеса, да и у представителей среднего и малого стоит на втором месте. Это понятно – IaaS прежде всего ассоциируется именно с предоставлением по сервисной модели виртуальных серверов.

Логично, что в срезе отраслей услуга чаще всего используется разработчиками ПО и ИТ-оборудования, самыми продвинутыми в плане ИТ клиентами, давно осознавшими преимущества сервисной модели. Отсюда же высокая среди потребителей услуги доля операторов связи. Эластичность предоставления сервиса и отсутствие необходимости держать свой ИТ-персонал на многочисленных точках делают услугу востребованной у предприятий оптовой и розничной торговли, нагрузка на ИТ-инфраструктуру которых связана с сезонными подъемами и спадами.

Эволюция спроса

Запросы на облачные сервисы меняются по мере развития бизнеса. Для малого бизнеса услуга восстановления после аварии (DRaaS) стоит слишком дорого, средний понимает важность непрерывного функционирования бизнеса и готов платить за него облачным провайдерам, а крупный проходит через эту стадию, затем разворачивает свои системы DRaaS и опять теряет интерес к данному сегменту облачного рынка. Схожая ситуация с услугой «виртуальный сервер GPU» – поставивший на поток исследования в области машинного обучения и искусственного интеллекта крупный бизнес предпочтет работать на своих ИТ-мощностях.

Прямо связан с масштабом бизнеса спрос на услуги в области безопасности. Предприятия малого бизнеса не могут позволить себе существенных инвестиций в эту сферу, да и внимание к ним со стороны злоумышленников не так велико. Как следствие, востребованность средств обеспечения безопасности у них низкая: по данным того же исследования, защиту от DDoS-атак среди используемых услуг отметили 19,4% респондентов этой категории, а защиту веб-приложений – 11,1%. Средний бизнес уже готов инвестировать в безопасность (27% – в защиту от DDoS-атак, 20% – в защиту веб-приложений), а больше всего интереса проявляет крупный бизнес (по 33,3% к обеим группам услуг).

Вопросами безопасности сильно озабочены операторы связи, что объясняется чувствительностью их бизнеса к прерыванию, когда даже кратковременные простои в работе серьезно сказываются на репутации компании, а в условиях жесткой конкуренции увеличивают отток клиентов. На операторов чаще обращают внимание регуляторы, поэтому многие из них пользуются услугой «облако, защищенное согласно ФЗ-152» (ее отметили 27,3% опрошен-

ных) – столь же востребована защита персональных данных лишь в медицине.

Другое следствие того, как важна для операторов непрерывность предоставления услуг, – частое, в два раза чаще, чем у следующих за ними по этому параметру банков, обращение к дорогому сервису DRaaS, который в России только начинает набирать базу пользователей.

Пока невысок интерес к услуге Kubernetes-as-a-Service (ее отметили 7,2% респондентов, см. рис. 1). Эта технология достаточно новая, и ее преимущества многим потребителям до конца не понятны. Услуга почти не находит спроса в таких консервативных отраслях, как транспорт и промышленность, зато неожиданно востребована в медицине: более поздний старт процессов цифровизации в отрасли обусловил, по всей вероятности, отсутствие инерции у ИТ-служб и внедрение сразу новых технологий.

Выбор облачного провайдера

Богатый ассортимент – дополнительная проблема для покупателя. С ней сталкиваются все посетители супермаркетов. На рынке IaaS конкуренция высокая, и выбрать облачного провайдера потенциальному клиенту нелегко.

Среди критериев выбора облачного провайдера на первом месте находится обеспечение высокого уровня безопасности данных – его считают очень важным 72% респондентов (рис. 2). Повышенное беспокойство по поводу безопасности данных в облаке – характерная особенность российского рынка. Впрочем, с течением времени тревоги утихают, и появляется понимание, что в облаке под присмотром профессионалов в области ИБ безопасность зачастую выше, чем на предприятии, не имеющем возможности оплачивать труд высококвалифицированных специалистов. Однако облака бывают разные. И клиент хочет понимать, что происходит в случае сбоя или пожара в ЦОДе, ему нужна прозрачность (мнение 61% респондентов).

Важна и прозрачность тарифов на услуги (60%) – неприятно узнавать, что кто-то заплатил за ту же облачную услугу значительно меньше. Конечно, ценообразование может быть сложным, напри-

мер, как у AWS, но в любом случае оно должно быть понятным, пусть даже для учета всех тонкостей надо приложить много усилий.

Конкуренция в наиболее освоенных клиентами сегментах базовых IaaS-услуг на российском рынке уже серьезная. Клиенты хорошо понимают базовые услуги, провайдеры накопили достаточную экспертизу: умеют эти услуги продавать и обеспечивать их поддержку. Но если говорить о более широком наборе сервисов, то здесь картина пока другая. Только небольшой части провайдеров, прежде всего крупным, удается планомерно расширять ассортимент и предоставлять клиенту понятный и прозрачный интерфейс взаимодействия.

Наиболее важным направлением развития рынка видится совершенствование клиентского сервиса, более глубокая автоматизация взаимодействия с клиентами посредством личных кабинетов.

Популярность облачного бренда

Базовые облачные сервисы становятся типовыми. Основная масса игроков предлагает примерно одинаковый набор услуг, и для того чтобы покупатель остановился у вашего «прилавка», нужно вкладываться в бренд.

Дмитрий Горкавенко, директор по развитию iKS-Consulting, выделяет три уровня (этапа) становления и восприятия бренда. Первый, базовый, уровень характеризуется обязательными атрибутами: высокая доступность сервиса (минимум 99,8%), соответствие законодательству, безопасность клиентских данных и др. Эти атрибуты должны иметь все компании, стремящиеся стать брендами в категории «облачный провайдер».

Второй уровень включает измеряемые атрибуты: количество вычислительных ядер, объем диска, пропускная способность канала доступа, длительность тестового периода, скорость реакции службы поддержки и т.п. Значение того или иного атрибута – например, цена в пересчете на 1 Гбайт, продолжительность тестового периода и пр. – определяет привлекательность предложения.

«Обязательные и измеряемые атрибуты – это этапы базовой узнаваемости и продуктовой конкуренции. Как правило, на этих этапах дискуссии о том, зачем данные атрибуты нужны облачному провайдеру, где заканчивается узнаваемость и начинается бренд, не возникает», – отмечает эксперт iKS-Consulting.

На третьем уровне в дело вступают привлекательные («восхищающие») атрибуты, чаще всего неожиданные для клиента. Они, как правило, не присутствуют у других игроков и служат основным инструментом для отстройки от конкурентов и эмоциональной привязки клиента (лояльности). При типовом продукте и отсутствии экономического и управленческого смысла инвестировать в «собственный код» такие атрибуты проще всего реализовать с помощью клиентского сервиса. Примеры «восхищающих» услуг: оперативное и доходчивое информирование клиента в случае сбоя, выделение персонального менеджера для решения интересующих клиента вопросов в удобное для него время, страхование рисков простоя, включая упущенную прибыль, в надежной страховой компании.

По мнению Д. Горкавенко, российский рынок IaaS уже завершил этапы 1 и 2: «Облачные провайдеры обзавелись обязательными (в понимании клиентов) атрибутами, сформировалось более или менее однородное их восприятие, а некоторые аргументы – такие как “безопасность в облаке часто выше, чем на своей инфраструктуре” – позволили привлечь новых заказчиков, которые три-четыре года назад переход в облака не рассматривали».

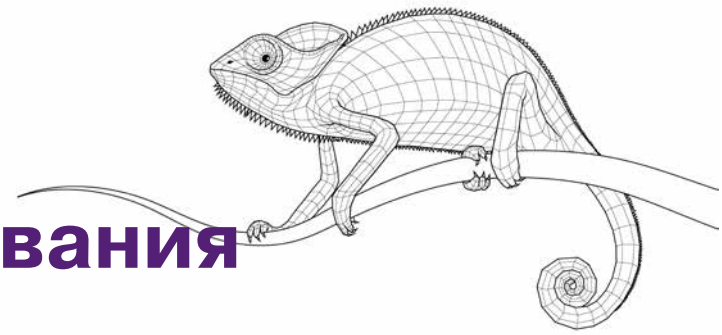
«К 2020 г. большинство провайдеров сформировали тарифные линейки, отслеживают тарифы конкурентов и адаптируются к их изменению. В таком виде рынок может существовать достаточно долго, до появления игроков, претендующих стать новыми лидерами рынка», – добавляет он.

Эксперты iKS-Consulting ведут рейтинг узнаваемости брендов облачных провайдеров среди компаний крупного бизнеса. По состоянию на май 2020 г. в первую десятку входят такие игроки, как «Ростелеком», Softline, Active Cloud, CloudMTS, DataLine, One Cloud, КРОК, «ИТ-Град», «Облакотека». Различия в результирующих показателях участников рейтинга небольшие, лидеры уже не раз менялись и с высокой вероятностью будут меняться и в дальнейшем.

Прогнозы и перспективы

«2020 г. с коронавирусом, скачками цен на нефтяном рынке, новыми премьером и главой профильного министерства (цифрового развития, коммуникаций и связи. – *Прим. ред.*) – подходящее время для передела облачного рынка в условиях общей неопределенности, – полагает Д. Горкавенко. – Сегодня при скромных инвестициях в коммуникационную стратегию можно построить бренд облачного провайдера со всеми обязательными атрибутами в аудитории крупных корпорантов и успешно развивать тарифную и продуктовую линейки».

...Все плохое рано или поздно заканчивается, и бизнес после эпидемии восстановится. Появятся новые заказчики, но бороться за них надо начинать уже сейчас. Преимущества получат те, кто не просто перетерпел тяжелые времена, а был активен, развивал сервисы, клиентскую базу и продвигал свой бренд в целевые аудитории. ИКС



Цифровизация как тактика выживания

Пандемия «приземлила» процессы цифровой трансформации – для все большего числа компаний из модной стратегии она превращается в тактику выживания. А «нагрузочное тестирование» ИТ-моделей и систем выявило узкие места и уточнило приоритеты развития.

Александр Барсков

Мода на цифровую трансформацию началась пару лет назад. Писались методички, разрабатывались стратегии, вводились новые должности (директора по цифровой трансформации, CDO), но далеко не все четко понимали, зачем. Пандемия вмиг ответила на этот вопрос. Там, где уже были внедрены современные ИТ, оцифрованы процессы и реализованы онлайн-сервисы, переход на работу в новых условиях произошел безболезненно. Тем же компаниям (отраслям), которые застряли в доцифровой эпохе, пришлось тяжело. И еще более актуальным стал выглядеть прогноз, предрекающий исчезновение около 40% существующих компаний в результате цифровой революции.

Сегодня важно оценить, как события 2020 г. изменят тактику и стратегию цифровой трансформации, как повлияют на модернизацию ИКТ-инфраструктуры. Одно из первых серьезных исследований этих вопросов в России, выполненное совместно iKS-Consulting и Intel, показало существенное влияние пандемии на ИТ-процессы в компаниях, а также выявило основные приоритеты развития ИКТ-инфраструктуры.

Парадоксы трансформации

Надо сразу сказать, что цифровая трансформация является одним из основных приоритетов бизнеса в России. Практически половина опрошенных компаний сообщила, что проводила оценку влияния цифровых технологий на бизнес. Больше всего таких компаний оказалось в медицине и фармацевтике, ТЭКе, транспорте и логистике.

Но удивительно, что в ряде отраслей количество компаний, утвердивших «единую стратегию цифровой трансформации бизнеса», превышает число тех, которые оценили влияние цифровых технологий на сам бизнес. Скажем, в сегменте финансовых организаций 55% опрошенных компаний уже утвердили стратегию, но только 45% разобрались, как цифровизация влияет на бизнес. В промышленности доли таких компаний соотносятся как 45% и 35%, в торговле – 58% и 33%, а в ТЭКе – 73% и 55%. Получается, что формальная сторона вопроса (утверждение стратегии) доминирует над фактическим пониманием пользы цифровизации.

В том же ТЭКе 64% опрошенных компаний имеют отдельное подразделение или сотрудника (например, CDO), отвечающего за цифровую трансформацию бизнеса. В банках и промышленности этот показатель находится на уровне 40%, а в медицине и фармацевтике лишь 29%. «Одной из основных проблем низкой доли цифровых кадров является необходимость существенной переподготовки персонала и дефицит специалистов на рынке. Как правило, цифровой трансформацией занимаются ИТ-директора и другие сотрудники, связанные с ИТ», – отмечает Денис Патрикеев, ведущий консультант iKS-Consulting.

Именно отсутствие квалифицированных кадров названо участниками опроса основным риском для цифровой трансформации (на это указали 29%). Также в первой пятерке рисков – недостаток финансовых средств, отсутствие единого понимания целей и процесса трансформации, непонимание ее эффекта/преимуществ и проблемы информационной безопасности.

Среди компаний, успешно проводящих стратегии цифровой трансформации в жизнь, аналитики выделяют КАМАЗ, «Почту России», «Сибур». Например, «Сибур» реализует концепцию «цифрового завода», которая предусматривает цифровизацию производственных и логистических процессов. На производстве внедряются аналитика с целью предиктивного обслуживания оборудования, цифровые двойники в железнодорожной логистике, позволяющие оптимизировать процесс перевозок, а также системы машинного зрения и беспилотные летатель-

▲ **Рис. 1. Факторы влияния пандемии и противоэпидемических мер на деятельность компаний**

ные аппараты для мониторинга производства и проведения технических осмотров. Все это помогает компании сокращать расходы и снижать риски промышленной безопасности.

Максимальный эффект, по мнению представителей 42% компаний, даст такое направление цифровой трансформации, как управление на основе данных. Также существенное влияние окажут цифровизация производственных процессов и развитие новых бизнес-моделей.

Влияние пандемии

Очевидно, что пандемия COVID-19 и меры, принятые Роспотребнадзором и Минздравом России, оказали существенное влияние на ИТ-процессы в компаниях. Это признали более 50% предприятий всех отраслей экономики. Например, в ТЭКе таких оказалось 64%, а в медицине и фармацевтике – 71%.

Главный фактор такого влияния – конечно, переход на удаленную работу (рис. 1). Это значительно увеличило нагрузку на ИТ-инфраструктуру, потребовало наращивания ее емкости. Почти каждой десятой компании пришлось временно приостановить основную деятельность.

«Компаниям, которые и раньше практиковали работу из дома, было, конечно, проще расширить инфраструктуру. Мы, например, имели опыт функционирования в таком режиме (наши сотрудники могут работать удаленно, а некоторые делают это на постоянной основе), но перевести на “удаленку” 100 тыс. человек – совсем другое, – рассказывает Сергей Жуков, директор по развитию бизнеса с государственными заказчиками в России и странах СНГ компании Intel. – Задача, которую пришлось решать экстренно, вызвала всплеск нагрузки на цифровые и сетевые ресурсы. Это привело к ощутимому росту потребления сервисов, став вызовом для телеком-сектора и облачных провайдеров. В основном они справились, и положительный опыт, который получили потребители, останется с нами».

В условиях неопределенности, в том числе относительно второй волны роста заболеваемости, трудно оценить, как пандемия повлияет на расходы на цифровизацию и ИТ-бюджеты в частности. Некоторые компании из нефтегазовой и банковской отраслей отметили, что расходы увеличились, отчасти в связи с организацией дополнительной инфраструктуры для VDI. Но значительная часть респондентов указала, что затраты остались на прежнем уровне. «Полноценно определить влияние COVID-19 на ИТ-бюджеты компаний станет возможным к концу 2020 г., когда компании подведут итоги года», – считает Д. Патрикеев.

Подавляющее большинство компаний (82%) полагают, что режим удаленной работы (пусть и частичный) сохранится и после пандемии COVID-19 до конца 2020 г. Правда, в самом вопросе заложен оптимистичный сценарий завершения пандемии еще в текущем году. «Пандемия осложнила процессы ведения бизнеса части компаний, возвращение к базовым показателям, которые были до нее, займет в среднем 6–12 месяцев», – прогнозирует эксперт iKS-Consulting.

ИКТ-инфраструктура: адаптивность на первом месте

Базис любой цифровизации – современная ИКТ-инфраструктура. Основными направлениями ее развития участники опроса назвали облачные вычисления, цифровой документооборот и безопасность ИТ-инфраструктуры (рис. 2). В то же время распределенная edge-инфраструктура, суперкомпьютеры и блокчейн оказались для респондентов на данном этапе неактуальными.

«Пандемия продемонстрировала наиболее узкие места ИТ-инфраструктуры, ее болевые точки. Компании их идентифицируют и будут соответствующим образом развивать сервисы, инфраструктуру, – считает С. Жуков. – Стало очевидно, что ИТ-инфраструктура становится критичной практически для любого бизнеса, и нужно продумывать все ее элементы в комплексе: ЦОДы и серверы, сети, производительность конечных устройств». Например, в ситуации, когда у сотрудника нет возможности вызвать ИТ-специалиста домой, необходимы решения для удаленного управления компьютерным парком.

«Пандемия еще раз показала, что мы движемся к цифровому миру, где требуются сбалансированные решения, определяемые сочетанием возможностей сетевой и вычислительной инфраструктуры и системы хранения. Если одна

◀ Рис. 2. Приоритеты развития ИТ-инфраструктуры

из этих частей становится узким горлышком, вся система начинает проседать», – добавляет специалист Intel.

Выделение респондентами в качестве основного приоритета развития облачных вычислений хорошо понятно. Именно облачная модель обеспечивает высокую степень адаптивности, которая важна не только для эффективной работы, но и для выживания компаний в нынешних условиях.

В целом, как показывает опыт компаний с развитой цифровой экосистемой, в основе быстрого и успешного внедрения инноваций лежат именно облачные технологии. Они позволяют быстрее запускать новые проекты и масштабировать существующие. В то же время растущая активность бизнеса по внедрению digital-проектов служит важным драйвером роста рынка облачных услуг.

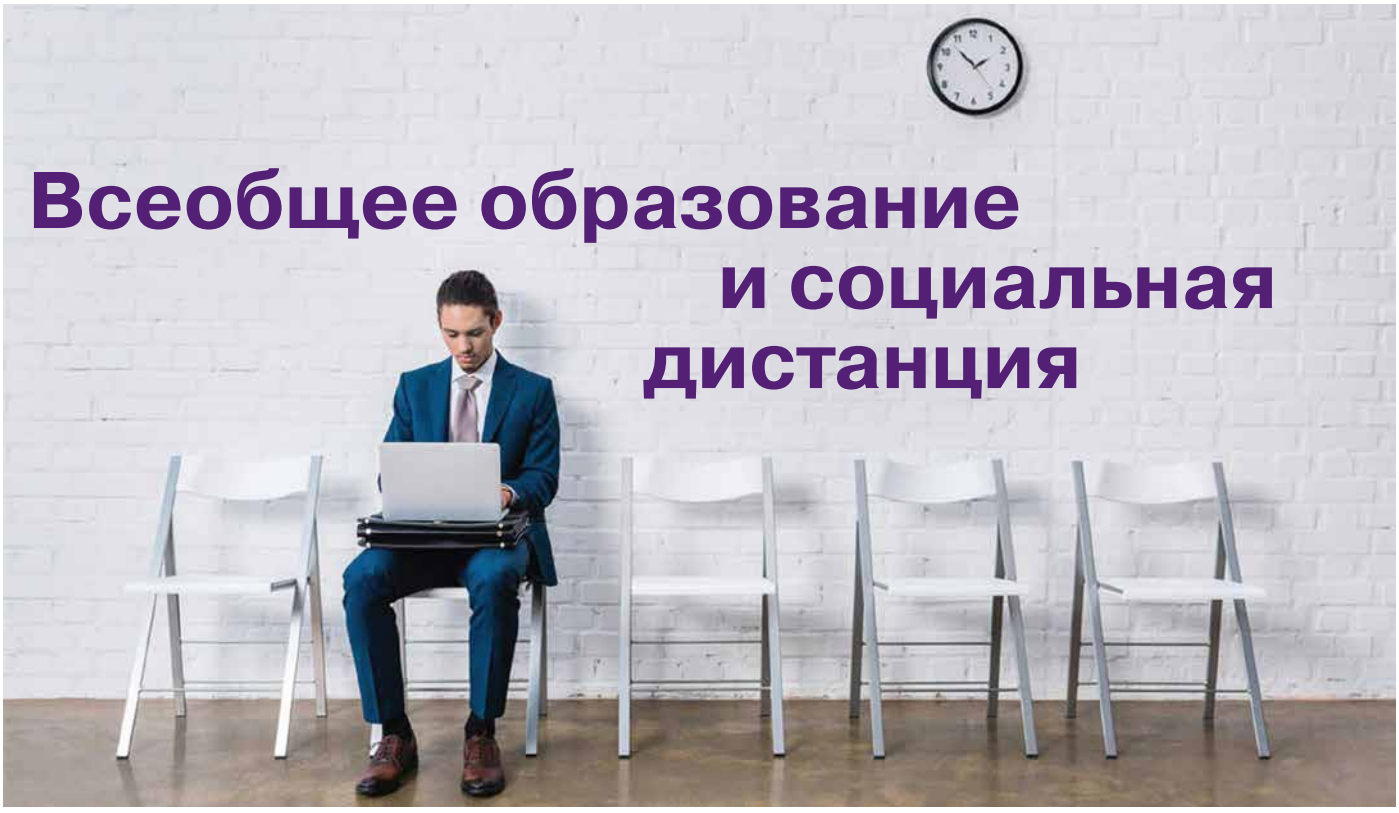
Этот рынок в 2018–2019 гг. стабильно увеличивался примерно на четверть ежегодно, и в 2019 г. его объем достиг порядка 86 млрд руб. (данные iKS-Consulting). Как отмечают представители крупнейших облачных провайдеров, в первой половине 2020 г. рост спроса на облачные услуги со стороны подавляющего числа сегментов экономики продолжился. При этом в силу сложившихся обстоятельств в первую очередь спрос увеличивался на решения, позволяющие:

- организовать удаленную работу сотрудников;
- построить эффективные методы коммуникации персонала;
- организовать хранение большого объема документов, архивов, баз данных;
- реализовать быстрое предоставление вычислительных ресурсов по требованию.

К тому же кризисные явления на фоне пандемии и нестабильных рынков подталкивают компании активнее искать новые пути сокращения издержек, что также приводит к росту спроса на облачные услуги.

«По сути произошло тотальное комплексное нагрузочное тестирование сложившихся моделей ИТ-инфраструктуры. Люди увидели и оценили на практике имеющиеся решения и сделают выводы, например, стоит ли отдавать часть нагрузки в облако или лучше строить свою инфраструктуру. Тренд на цифровизацию, модернизацию и построение гибридных систем останется. При этом специфика гибридизации (что оставлять в своем ЦОДе, а что отдавать в облако) будет зависеть от вертикали, от компании, от типа нагрузки: каждый увидел узкие и неустойчивые места в своей инфраструктуре и будет их оптимизировать», – отмечает С. Жуков.

Эксперты полагают, что во второй половине 2020 г. рынок облаков в России будет развиваться еще динамичнее. Компании не только увеличат потребление классических IaaS-сервисов, что позволит им сократить финансовые издержки, но и начнут более активно использовать PaaS-услуги. Благодаря такому подходу можно максимально эффективно и быстро трансформировать корпоративные ИТ-системы, провести их адаптацию для облака, получить реальные экономические выгоды и ускорить запуск новых продуктов и сервисов. ИКС



Всеобщее образование и социальная дистанция

Андрей Шолохов, директор департамента национальных проектов, Softline

Противоэпидемические меры социального дистанцирования вынудили школы, колледжи, университеты перейти в режим удаленного надомного обучения, к которому они в целом оказались не готовы, и споры о дистанционном массовом образовании разгорелись с новой силой.

Уже сейчас понятно, что технологии в образовательном процессе используются как «цифровые костыли» для того, чтобы так или иначе закончить учебный год и с сентября начать новый без отягощающих эпидемических обстоятельств.

При этом многие, особенно те, кто работает в сфере информационных технологий, видят в текущей ситуации возможность перейти к повсеместному широкому использованию дистанционного образования, заменив классическую школу, подобно тому, как покупки через интернет изменили торговлю. Но, открывая для себя «голубой океан» новых поставок цифрового оборудования и инфраструктуры для сферы образования, мало кто задается вопросом о критериях эффективного применения дистанционного образования на практике.

Дистанция застала школу врасплох

Повсеместный переход школ и вузов на дистанционное обучение – мера во многом вынужденная, служащая сиюминутным целям: позволить детям в условиях режима самоизоляции завершить учебный год. Никто не предполагал такого развития событий и, следовательно, не готовился к нему. Организованные онлайн-сессии выявили многочисленные проблемы. Например, уровень компьютерной грамотности школьников, их родителей и самих преподавателей существенно разнится и часто оставляет желать лучшего. Более того, в некоторых семьях нет ни стационарного компьютера, ни ноутбука. Родители были вынуждены ходить в школу к определенному времени, чтобы получить задания для своих детей или же передать на проверку тетради с выполненной домашней работой.

Из разных субъектов РФ поступает информация о сложностях с подключением к интернету из-за резко возросшей нагрузки на каналы связи. Скажем, на платформе онлайн-образования одновременно смотрят и слушают лекции около тысячи учеников. А ее возможности позволяют обслуживать только 50 человек. Наши технические мощности для организации дистанционного обучения не были рассчитаны на такое количество пользователей.

Власти всех уровней понимают масштаб проблемы и стараются по возможности исправлять ситуацию. Руководители некоторых регионов всерьез задумались о закупке доступных ноутбуков для школьников, семьи которых не имеют

собственных устройств. Параллельно идут переговоры с провайдерами об обеспечении бесперебойной интернет-связи. Сами школы активно тестируют площадки для онлайн-занятий. К примеру, в Москве часть учебных заведений по рекомендации городского Департамента образования активно использует ресурс «Московская электронная школа». Правда, его функционал и технические возможности устраивают не всех. Поэтому несколько школ выбрали работу на внешних платформах, среди которых наиболее популярны Google Hangouts, Zoom и Google Classroom.

Конечно, при наличии средств и возможности физической поставки инфраструктуры технические проблемы можно решить, но работающую методологию дистанционного обучения предложить в короткие сроки просто невозможно.

Цифровые надежды

Сложно разворачивающаяся для школ и университетов «битва за дистанцию» вызывает вопросы к стратегии развития системы образования, которая подразумевала перевод части учебного процесса в виртуальную среду.

До недавнего времени инновации внедрялись в отдельных учебных учреждениях, располагающих достаточными финансовыми и кадровыми ресурсами. При этом процесс часто был бессистемным – учебные заведения приобретали разрозненное ПО и оборудование вне единой концепции. Массовое внедрение цифровых технологий в образование началось со стартом национальных проектов «Образование», «Наука» и федерального проекта «Кадры для цифровой экономики» в прошлом году. И школы, и вузы стали комплексно подходить к реализации проектов в области цифровой трансформации.

Системы e-learning действительно востребованы образовательными учреждениями, но до настоящего времени они применялись преимущественно как дополнение к очному учебному процессу (дополнительное образование, повышение квалификации, обучение детей с ограниченными возможностями и т.д.). При грамотном подходе к внедрению и в связке с системами прокторинга, которые позволяют анализировать степень вовлеченности учащихся и контролировать соблюдение правил во время заочных тестирований, они могут достаточно эффективно решать задачу перевода части (при необходимости – большей части) учебного процесса в онлайн.

В трансформации высшего образования заинтересованы как образовательные учреждения, так и работодатели, которые хотят влиять на подготовку высококвалифицированных кадров для дальнейшей работы. В частности, Softline уже много лет оказывает технологическую и консультационную поддержку учебным заведениям в процессе внедрения инноваций, в том числе компонентов дистанционного обучения.

Социальная среда как ключевой фактор успеха массового образования

Текущая практика дистанционного обучения показывает, что большинство детей, подростков и даже взрослых быстро теряет интерес к занятиям, если нет живого общения. Почему это происходит? В качестве одной из причин некоторые эксперты называют отсутствие специализированного контента.

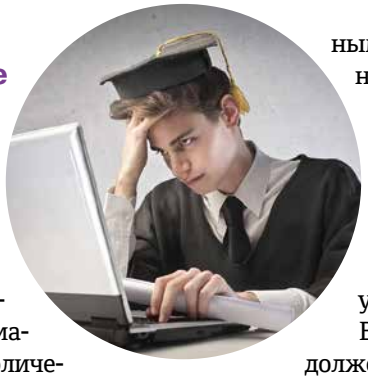
На многочисленных информационных ресурсах в интернете можно посмотреть и прослушать лекции по самым разным областям знаний. При этом обращается к лекциям только тот, кому интересна содержащаяся в них информация. Однако надо четко понимать, что образование – это не потребление контента по выбору, здесь присутствует элемент обязательности.

Успех классической школы основывается на том, что в процессе обучения задействуются все три типа мышления ученика или студента. При этом идет не только усвоение абстрактной новой информации и встраивание ее в индивидуальную картину мира, но и фактически овеществление изучаемого методом погружения в совместную деятельность, а также формируется эмоциональное отношение к предмету изучения вплоть до реакции «нравится/не нравится».

И, самое главное, обучение в сложившемся коллективе задействует социальное мышление, когда поведение на уроке напрямую влияет на социальную значимость ученика и отношение к нему одноклассников. В здоровом сообществе с высокой ценностью знаний и умением обучаться социальный эффект намного более важен для успеха образовательной деятельности, чем просто умение работать с информацией.

Утверждение, что будущее исключительно за дистанционным обучением и текущая эпидемическая ситуация серьезно подтолкнет человечество к образовательной дистанции, равносильно утверждению, что в дальнейшем все соревнования по бегу будут проводиться исключительно в мешках. Дистанционное образование задействует абстрактное и иногда эмоциональное мышление, но очень редко затрагивает социальный аспект.

Уверен, когда массовое образование сможет сбросить «мешки», оно это сделает и вернется к классической школе. Но остается важный вопрос: где место дистанции в массовом образовании, где она может принести дополнительную пользу?



Национальные проекты и дистанционное образование

Все ученики имеют разные навыки и стремление к обучению. Нельзя сказать, что классическая система образования не понимала и не использовала это. В качестве примера можно привести учебные заведения олимпийского резерва, физико-математические школы, специализированные классы с большим количеством предметов по отдельным направлениям.

Даже в национальном проекте «Образование» упор сделан не на изменении основного образовательного процесса, а на развитии системы дополнительного образования. Аналогом физико-математических школ сегодня выступают кванториумы для изучения инженерных наук, ИТ-кубы, помогающие получить цифровое образование, учреждения, подобные фонду «Талант и успех», позволяющие заниматься искусством, спортивными и естественно-научными дисциплинами, специальные мастерские с мощной научно-технической базой и даже научно-образовательные центры.

Все перечисленные центры дополнительного образования используют успешную практику классической школы, формирующей устойчивые группы обучающихся, а в процессе коллективной образовательной деятельности задействующей все возможности мышления учеников.

Упоминаются в национальном проекте «Образование» и онлайн-занятия, например «Проектория» и «Уроки настоящего». Но они не интегрированы в образовательный процесс и по сути являются аналогом научно-популярных программ на телевидении или в интернете. Возникает непраздный вопрос: какие шаги необходимо предпринять в рамках нацпроекта, чтобы более активно использовать все возможности дистанционного образования?

Первый и самый очевидный шаг – это разработка схемы дистанционного обучения на базе кванториумов, ИТ-кубов, мастерских. Идея создать мобильные кванториумы имеет право на жизнь, но даже эти машины не могут приехать к каждому способному ученику. Дополнительное образование имеет большую свободу для эксперимента и ошибки.

После того как дистанционное образование будет опробовано на базе систем дополнительного образования и появятся методики применения, можно внедрять его элементы в общеобразовательных школах и вузах.

Усидчивые, самостоятельные школьники, готовые и способные глубоко изучать отдельные предметы, могут быть частично переведены на дистанционное обучение по специализированным программам с помощью удаленной образовательной инфраструктуры. И тогда важные задачи нацпроекта «Образование», связанные с формированием индивидуальных образовательных траекторий, могут быть решены на более высоком практическом уровне, чем сейчас.

В высшей школе подобный подход должен привести к появлению виртуальной академической мобильности. Как в свое время рынок программного обеспечения выделился из рынка компьютерного оборудования и стал существенно менять нашу жизнь, так и рынок академического контента должен выделиться из рынка учебных заведений. Вузы должны иметь возможность приобретать необходимый контент извне в том числе за государственные деньги, а студенты – официально заменять обучение некоторым предметам в родном вузе дистанционным прохождением курсов в сторонних образовательных учреждениях и таким образом достраивать свои образовательные траектории.

В национальном проекте важно учесть необходимость устранения цифрового неравенства. Полноценное внедрение новых технологий, включая платформы дистанционного обучения, могут себе позволить в основном наиболее коммерчески успешные учебные заведения (речь прежде всего о крупных вузах). Остальные вынуждены внедрять решения, находящиеся в свободном доступе, которые часто не обладают достаточным функционалом. Поскольку скорость армии определяется самым тихоходным подразделением, государственные усилия обеспечить оптимальный уровень цифровой инфраструктуры для всех вузов страны должны существенно нарастить возможности системы высшего образования в целом.

Самое главное, такая важная государственная инвестиционная деятельность, как национальные проекты, в том числе в области образования, должна перейти на более гибкие методы управления. Жизнь снова показала, что, к сожалению, недостаточно разработать неизменные планы до 2024 г. Нужен открытый, понятный механизм коррекции таких планов в зависимости от промежуточных результатов.

Речь идет не о том, чтобы часть средств перебросить на более актуальные в данный момент задачи. И правительство, и общество уже осознали, что подходы к дистанционному образованию в рамках национальных проектов не были в должной мере проработаны. Именно для того чтобы накопленный опыт удалось превратить в плодотворную практику, требуется регулярная адаптация мер государственной поддержки, заложенных в национальные проекты. ИКС

АНАЛИТИЧЕСКИЙ ОТЧЕТ

«Российский рынок коммерческих дата-центров 2019–2024»

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 2020–2024 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.

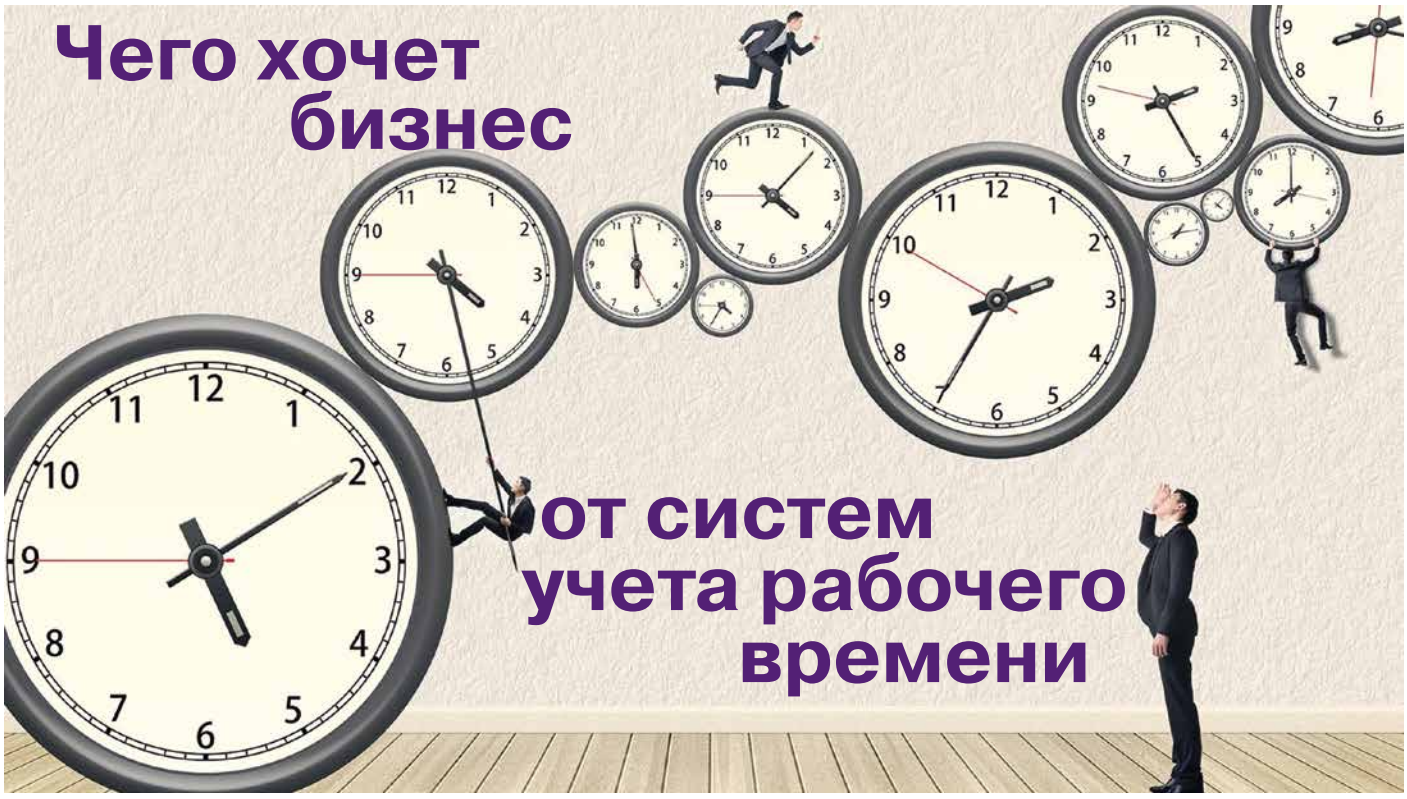
Параметры отчета

- 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

Чего хочет бизнес от систем учета рабочего времени



Александр Бочкин, генеральный директор, «Инфо-максимум»

В удаленном режиме сотрудники работают в среднем на 2,5 часа в день больше. Умножьте на количество сотрудников и стоимость часа их работы. Выгода для бизнеса очевидна.

Эксперты считают, что мировой ВВП имеет шансы вернуться на докризисные позиции не раньше IV квартала 2021 г. Для многих рецептом выживания в сложившейся ситуации стал переход в онлайн. В результате одними из самых популярных ИТ-решений оказались системы учета рабочего времени. Это было предсказуемо: предыдущий «расцвет» подобного ПО пришелся на время кризиса 2014-го, когда управленцы искали надежные способы экономии и повышения собственной эффективности в непростых условиях.

Системы учета времени сейчас

Современный софт для учета рабочего времени и загруженности персонала предоставляет статистику для подробного анализа. Системы показывают продуктивность персонала, оценивают степень его загруженности, способны зафиксировать переработки или неправильное разделение обязанностей, которое ведет к простоям.

Важно не только зафиксировать показатели, но и проанализировать их:

- выяснить, сколько времени сотрудник тратит на рабочую задачу;
- сравнить данные по отделу;
- найти причины срыва дедлайнов;
- определить процессы, которые занимают слишком много времени.

Возможно, придется организовать дополнительное обучение или провести кадровые ротации.

«Внимательный» софт поможет определить сотрудников, которые задумываются об увольнении, зафиксировав их активность на сайтах поиска работы. Все эти данные нужны для планирования и грамотного принятия управленческих решений, повышения эффективности.

Однако больше всего подобные системы ориентированы на поиск резервов времени: время – деньги, время – возможности. Согласно исследованиям нашей компании, на «удаленке» сотрудники тратят на работу в среднем на 2,5 часа в день больше. Умножьте на количество сотрудников и стоимость часа их работы. Ощутили разницу?

Чего хочет бизнес

Если кратко, то бизнес хочет выжить: не растерять клиентов и удержать собственные позиции. Мало кто планирует расширяться в ближайшие несколько месяцев, проекты замораживаются, заключение сделок откладывается.

Среди самых популярных вопросов, которые задают те, кто впервые столкнулся с учетом рабочего времени и анализом загруженности персонала, можно выделить следующие.

1) Нужна видео/аудиофиксация работы сотрудника. Как это сделать?

Это один из самых первых вопросов, и его популярность не случайна. Многие системы учета рабочего времени позиционируются как «шпионы», некий «Большой Брат», который внимательно следит абсолютно за всем, что сотрудник делает на рабочем компьютере. Логично, что подход с фиксацией каждого шага и вздоха персонала может вызывать у работников дискомфорт и психологическое напряжение, формируя у людей ошибочные представления о таком софте. Некоторым руководителям важно действительно знать о сотрудниках все, поэтому они выбирают жесткие системы, оснащенные кейлоггером, видеофиксацией, записью аудио. Принятие таких мер – вопрос рабочей этики и юридической обоснованности, поскольку при видеозаписи или на скриншотах экрана могут промелькнуть личные данные или переписка сотрудника.

2) Что делать, если сотрудник работает на своей технике? Можно ли скрытно установить программу на его компьютер?

Поскольку не все работодатели могут обеспечить персонал рабочими ноутбуками, этот вопрос один из наиболее часто задаваемых. Домашний ПК – это личное пространство сотрудника, и устанавливать на него любой софт «тихой сапой» – в корне неверно. Специалист должен дать письменное согласие на установку программного продукта или же использовать какое-либо облачное решение, собирающее статистику исключительно в рабочее время.

3) Учитываются только нажатия клавиш и мышки?

В большинстве случаев – да, это основные показатели рабочей активности сотрудника. Как правило, фиксируется время, проведенное в активном (открытом на данный момент) окне. Это может быть как активная вкладка в браузере, так и программа или документ.

4) Какой функционал используется чаще всего?

Запросы клиентов индивидуальны. То, что обязательно для одного, находится в конце списка приоритетов другого. Тем, кто обращается к подобному ПО впервые, бывает сложно ориентироваться во всех его возможностях. Как правило, существует некий базовый функционал, которым обладают все уважающие себя системы учета:

- разделение отработанного времени на продуктивное и непродуктивное;
- отчет об использовании программ и вебсайтов каждым сотрудником;
- информирование о нарушениях норм (опоздания, прогулы, ранние уходы);
- формирование табеля с количеством отработанных часов.

«Удаленка» неэффективна?

Совместно с семью клиентами – пользователями облачных аккаунтов нашей системы мониторинга загруженности и учета рабочего времени – мы сравнили статистику за два месяца: февраль и апрель (месяцы, которые сотрудники провели полностью в офисе и полностью на «удаленке»). Суммарное количество отработанного времени в каждой компании значительно возросло – сотрудники стали работать больше в среднем на 2,5 часа (подтверждают эти цифры и международные исследования: по данным NordVind, в США рабочий день увеличился в среднем на 3 часа, в Европе – на 2 часа). Если нормальная продолжительность рабочего времени за неделю составляет 40 часов, то на «удаленке» этот показатель вырос до 51 часа.

Причин этому несколько:

- отсутствие переключения «работа/дом». Люди перестают воспринимать дом как место для отдыха;
- несбалансированное использование времени: особый акцент на работу в ночи и до утра, решение срочных/важных/несрочных/неважных дел практически в любое время суток. Ведь «все рядом, почему бы нет»;
- отвлечения. У многих сотрудников есть маленькие дети, требующие внимания, или шумные соседи. Это мешает сосредоточиться на рабочих задачах.

В каждой из рассмотренных нами компаний продуктивность выросла, особенно среди руководящего состава. Это обусловлено необходимостью усилить контроль и управление, постоянными коммуникациями и более тщательным планированием. Однако мы склонны считать эффект временным. Главный недостаток такой повышенной самоотдачи – накопление хронической усталости, которая в дальнейшем может повлиять на скорость и качество выполняемых задач и понизить эффективность работы. Переработки при этом сохранятся.

5) Можно ли обмануть систему и нарушить корректность собранной статистики?

Опасение понятно, но сегодня практически все разработчики систем учета рабочего времени гарантируют достоверность данных мониторинга. Пользователь, на рабочей машине которого действует такое ИТ-решение, без прав администратора не может отключить агента сбора статистики. Сотрудники самостоятельно вводят в систему информацию о том, чем занимались в тот или иной период времени вне работы за ПК: совещание, оформление документации, планерка и т.д. Как показывает опыт, не все добросовестно сообщают о своей занятости: кто-то может элементарно забыть, а кто-то намеренно ввести в заблуждение. Однако анализ даст итоговый расклад.

Система учета рабочего времени – лишь инструмент: интересы сотрудников и руководителей в ее использовании прозрачны. Коронавирус, удаленная работа – все это стало нашей обыденностью и изменило бизнес безвозвратно. И чем быстрее компания перестроится на «цифру» и внедрит ее в свою работу, тем проще ей будет развиваться в дальнейшем. ИКС

Как обеспечить безопасность бизнеса на «удаленке»

Мурад Мустафаев, руководитель службы информационной безопасности, «Онланта» (ГК ЛАНИТ)

В обычной офисной жизни сотрудникам несложно соблюдать корпоративные правила информационной безопасности, а ИТ-службе – создавать для этого необходимые технические условия и осуществлять контроль. Но при переходе на удаленную работу появляется много нюансов.

Когда сотрудники работают из дома, ИТ-служба не может настроить их личные компьютеры в соответствии с требованиями информационной безопасности компании; не все программное обеспечение, установленное на личном ноутбуке сотрудника, лицензионное; нет антивирусных программ, а если есть, то они, как правило, либо бесплатные с ограниченными возможностями, либо работают в ознакомительном режиме с ограниченным временем бесплатного использования.

В этой статье я расскажу о том, какие правила нужно ввести для сотрудников на «удаленке», чтобы снизить риски нарушения конфиденциальности корпоративных данных.

Корпоративная безопасность vs удаленная работа

В нашей привычной бизнес-жизни действуют стандарты информационной безопасности ISO 27001, используются лучшие мировые практики для достижения целей ИБ по защите информационных систем компании. Эти своды правил являются универсальными. Но можем ли мы обеспечить их выполнение в режиме удаленной работы и защитить корпоративные и личные устройства?

Ответственность

В офисе мы работаем с корпоративных устройств, а служба информационной безопасности защищает всю рабочую сеть с помощью средств защиты. О нарушениях правил ИБ сотрудником становится известно практически сразу – это позволяет принять необходимые меры и обезопасить инфраструктуру компании от угроз.

В удаленном режиме не все сотрудники работают с корпоративных ноутбуков. Поэтому отслеживать нарушение регламентов безопасности сложнее. В случае, если сотрудник работает на личном ноутбуке, важно реализовать ряд защитных мер, чтобы корпоративные данные не ушли вовне.

Что делать. Необходимо напомнить сотрудникам требования ИБ и усилить контроль: более пристально следить за SIEM-системой, тщательнее контролировать спам-систему, отбивки ИС, обеспечить согласование заявок с более глубоким контролем.

Разрешите сотрудникам использовать в удаленном режиме свои рабочие ноутбуки или VDI. Так вы точно будете уверены, что все ИБ-требования компании выполняются. Работа с личных устройств не гарантирует 100%-ной безопасности и соблюдения регламентов, поскольку эти устройства сложнее контролировать.

Управление активами

Компания – это живой организм, в котором ежедневно происходят изменения, данные о пользователях подвергаются постоянному анализу и актуализации. Это важно, так как пользователи должны следить за работоспособностью порученных им информационных активов, отвечать за соблюдение требований ИБ.

Что делать. У любого актива должен быть владелец, являющийся сотрудником организации. Сотрудник, ответственный за актив, может контролировать его как из офиса, так и удаленно. Главное – проверять уровень доступа.

При удаленном режиме работы необходимо отнестись к правам с особенным вниманием. Пользователям нужно объяснить, что доступ к информационным активам выдается после согласования руководством. Если доступ к активу отсутствует, нужно обратиться к администратору системы или в службу поддержки.

Классификация информации

Доступ к информации в зависимости от уровня ее конфиденциальности может быть общим или ограниченным. Есть конфиденциальная информация, доступ к которой разрешен только определенному кругу лиц в компании. Так должно быть в любой организации: если данные не относятся к общедоступным, доступ к ним необходимо категоризировать.

Что делать. Доступ к данным, как при офисном режиме работы, так и при удаленном, должен осуществляться с помощью матрицы доступа. Удаленный доступ должен быть организован посредством шифрованного VPN-канала с разграничением прав доступа, что гарантирует соблюдение принципа «у каждого свой доступ к необходимой информации».

Работа с персоналом

К сожалению, до сих пор часты ситуации, когда сотрудник долго скрывает, что подключался к информационным системам компании без соблюдений требований ИБ, потерял ноутбук или конфиденциальную информацию. В этом случае компания не может вовремя отреагировать на возникшие риски.

Каждый сотрудник должен быть ознакомлен с документами, которые описывают его должностные обязанности, и понимать, как вести рабочую деятельность в соответствии с требованиями ИБ, принятыми в компании. Работодатель обязан предупреждать сотрудников о возможной административной или уголовной ответственности в случае нарушения регламентов и правил информационной безопасности компании.

Что делать. При переводе сотрудников на удаленную работу стоит освежить в памяти основные аспекты информационной безопасности компании: разослать им требования ИБ и попросить относиться к корпоративным и конфиден-

циальным данным с особым вниманием, а также напомнить об ответственности. Возможно, стоит выпустить новые приказы и разъясняющие документы. В документах должна быть предусмотрена ответственность сотрудника в случае нарушения им требований ИБ в удаленном режиме.

За важные документы при работе с ними и их распространении ответственность несет сотрудник (даже если документы были взломаны злоумышленниками). О малейшем подозрении, что произошла утечка конфиденциальной информации, он должен незамедлительно сообщить сотрудникам службы ИБ.

Безопасность сети

Безопасность сетевой инфраструктуры напрямую зависит от обособленности сегментов сети. Часто в организациях нет сегментации сети, никто не может разобраться в информационных системах: какие ресурсы взаимодействуют между собой и по каким протоколам. При переводе сотрудников на удаленную работу начинаются проблемы с доступом, и компания простаивает.

Что делать. Для простого администрирования и контроля рекомендуется разделить сеть организации на несколько подсетей в соответствии с их особенностями (сеть управления, DMZ и т.д.) и ограничить взаимодействие между ними, разрешив только необходимый для работоспособности организации трафик. Сетевому специалисту следует вести журнал соответствия IP-адресов, открытых портов и используемых служб для каждого сетевого узла в инфраструктуре организации.

Сегментация позволяет разграничить права определенных групп пользователей и взаимодействие сетей. Например, менеджеры находятся в одной сети с доступом к определенным информационным системам компании, а группа экспертов имеет расширенные права доступа для администрирования и поддержки бесперебойной работы ИТ-систем. Таким образом снижается риск взлома «менеджерской» сети и доступа к административным ресурсам компании. Также разделение сетей способствует разграничению прав доступа к VPN, что позволяет в кратчайшие сроки перейти на удаленный режим работы, сохраняя все права доступа сотрудников к информационным системам.

Контроль доступа

Каждый сотрудник имеет права доступа к ресурсам, необходимым для выполнения должностных обязанностей. Сложность пароля, срок его годности, блокировка при бездействии, пересмотр прав доступа (при смене должности) – все это необходимо контролировать.

Что делать. Нужно организовать возможность сброса пароля сотрудника как из офиса, так и извне его. Доступ должен осуществляться исходя из матрицы доступа. Необходимо выработать политики блокировки доступа в случае обнаружения инцидента ИБ (аномального поведения системы, взлома, попыток перебора пароля и т.д.). Во время удаленной работы контроль за инцидентами ИБ должен быть усилен.

Обмен информацией

В офисе мы общаемся с помощью корпоративной почты, рабочих телефонов, а иногда можем подойти к коллеге и переговорить с глазу на глаз. Как быть во время удаленной работы? Конечно, невозможно не пользоваться мессенджерами, которые всегда под рукой. Просто запретить это делать бесполезно.

Что делать. К использованию некорпоративных ресурсов нужно подойти с умом и помнить азбучные правила: не забывать, что простая установка VPN-клиента и его верная настройка ими-

РЕКОМЕНДАЦИИ ЭКСПЕРТА

Влияние режима удаленной работы на SOC

Анна Михайлова,
системный архитектор, группа компаний Angara

Рекомендуем ИБ-аналитикам обратить внимание на следующие факторы:

1. Размылись границы рабочего дня. Многие корреляционные методики отталкиваются от офисного режима работы с различным дневным и ночным почерком активности, который в режиме удаленной работы изменился.

2. Изменения конфигурации оборудования и установка средств удаленного администрирования на ПК пользователей стали производиться намного чаще.

3. Сильно выросла активность вредоносного ПО, включая довольно старые его образцы.

4. Действие дополнительных средств защиты компаний от утечек, таких как внутренний сетевой периметр, запрет на подключение внешних устройств или использование личной электронной почты на ПК пользователя, в режиме удаленной работы может быть ослаблено. Поэтому инцидентам DLP-систем необходимо присвоить высокий приоритет.

Рекомендуется тщательно следить за целостностью конфигураций серверных компонентов: контролировать установку нелегитимного ПО на них, подключение по нелегитимным протоколам, особенно использующимся для объемной выгрузки данных (SMB, FTP) и т.д. Крайне важен мониторинг запросов в базы данных во избежание массовых утечек информации.

тирует ваше нахождение в офисе. Для коммуникаций можно задействовать мессенджеры, но никакой конфиденциальной информации при этом не передавать, вести диалоги с коллегами лишь о каких-то общих, неконфиденциальных вопросах.

Обмениваться «щепетильной» информацией нужно через почтовый клиент и другие защищенные корпоративные ресурсы – они для этого и созданы. Если сотрудник использовал для отправки корпоративной информации незащищенный ресурс, любой сотрудник ИБ-службы вправе возбудить инцидент.

Мониторинг

Конечно, за соблюдением требований, описанных выше, необходимо следить. Возбуждать инциденты ИБ и проводить расследования для привлечения сотрудников к ответственности. Такие меры служат не для наказания, а для повышения уровня безопасности компании и защиты корпоративных ресурсов от внешних атак.

Осуществлять мониторинг информационных систем компании, когда сотрудники находятся в офисе в одной сети, сложно. Но еще сложнее, когда они работают удаленно, особенно если нет настроенного мониторинга ИБ и потому затруднительно определить, исходит ли трафик от сотрудника компании и является легитимным или же это работа злоумышленника.

Что делать. Необходимо настроить мониторинг удаленных рабочих мест и следить за соблюдением требований информационной безопасности компании. В случае обнаружения угроз сразу же возбуждать инциденты и проводить расследования.

Инструменты безопасности

Для реализации предложенных мер обеспечения корпоративной безопасности можно порекомендовать целый ряд инструментов.

Аутентификация. Верно настроенные групповые политики в Active Directory для централизованного управления учетными записями пользователей. Двухфакторная авторизация путем использования сертификатов, токенов (физических/программных) и т.д.

Защита информационных ресурсов. Комплексы WAF (Web Application Firewall) для защиты веб-ресурсов компании от несанкционированных атак. Межсетевые экраны, сканирующие сетевой трафик веб-приложений и блокирующие нелегитимный трафик. Даже использование стандартных профилей (OWASP TOP 10) позволит неплохо обезопасить ваши ресурсы. Конечно, на первых этапах эти инструменты требуют к себе большего внимания для тонкой настройки, но это отличный продукт для защиты веб-ресурсов компании.

Сканирование ИС компании с целью выявления уязвимостей помогает вовремя обнаружить «дыры» в инфраструктуре и закрыть их. Совет: сканирование стоит проводить в нерабочее время, чтобы избежать повышения нагрузки на сеть.

Доступ к информации. VPN (Virtual Private Network) служит для доступа к корпоративным сервисам из внешней сети. Использование VPN обеспечивает доступ к ресурсам, не подключенным к сети интернет. Интегрированный VPN с Active Directory дополнительно обезопасит ваши соединения.

Не стоит забывать, что контролировать одно узкое горлышко всегда проще, чем открывать доступ в интернет всем системам компании.

Защита рабочих мест. Антивирусное программное обеспечение для обнаружения и профилактики заражения вирусами файловой или операционной системы.

DLP-системы (Data Leak Prevention), предотвращающие утечки информации из внутреннего периметра компании. Пригодны и для контроля рабочих мест вне офиса. Управление и контроль можно осуществлять централизованно.

VDI (Virtual Desktop Infrastructure), виртуальные рабочие столы. Служат для доступа к полноценному рабочему месту, для контролируемого доступа ко всем необходимым корпоративным ресурсам. Использование VDI в сочетании с двухфакторной аутентификацией – одно из самых безопасных решений для удаленной работы в корпоративной сети.

Мониторинг. Система SIEM (Security Information and Event Management) служит для сбора событий со всех информационных ресурсов компании. С помощью заданных правил SIEM-система умеет определять инциденты информационной безопасности. Позволяет осуществлять контроль в автоматическом режиме. Однако развертывание этого решения обходится достаточно дорого и в финансовом плане, и в плане трудозатрат: потребуются покупка самого решения, внедрение и настройка, работа специалистов отдела информационной безопасности.

При функционировании бизнеса в удаленном режиме (да и не только в удаленном) сотрудникам ИТ-службы не стоит надеяться на авось. Важно заранее продумать защиту и безопасный доступ к инфраструктуре компании. Не следует выстраивать систему безопасности, которая будет затруднять сотрудникам жизнь; необходимо использовать проверенные и качественные решения. Верно настроенные системы и внимательное отношение сотрудников к правилам безопасности – это 70% успеха в защите инфраструктуры компании от угроз информационной безопасности. ИКС

Безопасность коботов: распространенные мифы и реальность

Славой Мусилек, генеральный директор в Центральной и Восточной Европе, России и СНГ, Universal Robots

Благодаря наличию встроенных функций безопасности эксплуатация коллаборативных роботов не требует дорогостоящей и нередко громоздкой защитной инфраструктуры.

Помимо прибыльности производства необходимым условием успешности промышленного предприятия является безопасность персонала. Любая производственная травма или заболевание, развившиеся у сотрудника вследствие работы на предприятии, оцениваются в соответствии со строгими стандартами безопасности и отягощают компанию высокими дополнительными издержками. Чтобы избежать ситуаций, сопряженных с риском, с самого начала автоматизации производства промышленные роботы отделялись от работников с помощью нескольких защитных ограждений. Коллаборативные роботы (коботы), т.е. автоматические устройства, которые могут работать совместно с человеком для производства различных продуктов, полностью изменили правила игры. Их можно устанавливать на предприятиях малого и среднего бизнеса без защитной инфраструктуры, требующей больших затрат и занимающей ценное пространство.

Коботы могут быть легки и удобны в использовании, а их внедрение – интуитивно понятно. Программирование робота-манипулятора может выполняться в том числе с помощью прямого физического контакта с ним. Коботы активно используются в непосредственной близости от людей без каких-либо защитных ограждений. Однако такой подход требует полного контроля над скоростью, усилием, мощностью и импульсом, развиваемыми этими устройствами в процессе работы. Хотя они полностью соответствуют стандартам безопасности, с их эксплуатацией связано множество мифов. Рассмотрим самые популярные.

Роботы небезопасны без защитных ограждений

Это самый распространенный миф, который опровергается многими успешными примерами внедрения коботов в производство. Современные коботы имеют функции обеспечения безопасности, как встроенные, так и адаптируемые для конкретного заказчика. Они всегда имеют предустановленные функции аварийной остановки или остановки по требованиям безопасности. При этом пользователи могут настраивать скорость движения робота, диапазон вращения и угол поворота его шарниров, усилие, импульс, мощность, время остановки, расстояние до остановки и другие параметры.

На практике чаще всего настраивают скорость движения робота, так как она больше всего влияет на передачу усилия от робота к человеку в случае их взаимодействия. Пространственные ограничения также применяются достаточно часто. В последнее время все более популярными становятся датчики безопасности, позволяющие уменьшать скорость движения робота, если человек находится к нему слишком близко. Настройка конкретных параметров всегда зависит от заданной области применения кобота и условий производственного помещения.

Коллаборативные роботы всегда безопасны

Это другая крайность, и это мнение также не соответствует действительности. Комплексный подход требует, чтобы безопасным был не только сам робот-манипулятор, но и его рабочий инструмент. Так, если робот-манипулятор используется в сочетании с инструментом для резки

или сварки либо перемещает потенциально опасные предметы, он не может считаться безопасным, если не имеет внешних защитных ограждений. Сегодня множество производителей предлагают широкий ассортимент рабочих инструментов, и на эти компании возложена обязанность обеспечивать безопасность их работы. В будущем именно производители рабочих инструментов выйдут на первый план в установлении новых норм и стандартов безопасности для коллаборативных приложений.

Например, современные захватные устройства предназначены для перемещения предметов с точно заданным усилием, достаточным для захвата, но не превышающим необходимого уровня. Это позволяет свести к минимуму риск получения травмы при случайном взаимодействии манипулятора с рукой человека. Кроме того, производители коботов должны проходить обязательную сертификацию и их продукция должна быть признана безопасной для использования.

Чем больше робот по размеру, тем менее коллаборативным он становится

С началом производства коботов, обладающих повышенной полезной нагрузкой, безопасность их работы в одном пространстве с человеком обсуждается все более активно. Чем больше робот по размеру, тем выше его грузоподъемность, тем больше электроэнергии он потребляет для работы с материалом и тем более высокому риску, как считается, подвергаются операторы. На самом деле риск определяется не размером робота, а конкретным способом его применения и соответствующей ему настройкой параметров безопасности.

Некоторые способы применения роботов малого размера представляют бóльшую опасность, чем использование громоздких роботов. Например, самая компактная модель робота, оперирующего опасными веществами в лаборатории, может быть менее коллаборативной, чем более крупная по размеру модель, эксплуатируемая с иной целью в другой области применения. Использование крупногабаритных коботов для операций типа «взять и положить» или паллетирования в сочетании с корректно настроенным датчиком безопасности может считаться более коллаборативным. В непосредственной близости от оператора датчик безопасности замедляет движение кобота до уровня, позволяющего ему безопасно взаимодействовать с человеком. Например, неотъемлемой частью всех наших коботов являются настраиваемые параметры, которые позволяют упростить интеграцию датчиков безопасности.

Процесс настройки параметров безопасности слишком сложен

Как правило, коботы должны проходить сертификацию на соответствие уровню d эффективности защиты стандарта безопасности оборудования ISO 13849. В соответствии со спецификацией ISO/TS 15066 они позволяют проанализировать и оценить риски и требования во время установки. Хотя 80% из 42 тыс. наших коботов, работающих по всему миру, эксплуатируются без каких-либо внешних защитных ограждений, мы всегда рекомендуем провести анализ и оценку рисков для конкретной цели и способа применения кобота. Благодаря предустановленным режимам безопасности выбор параметров осуществляется легко и интуитивно. В некоторых случаях пользовательский интерфейс робота также позволяет задавать параметры безопасности интегрированных рабочих инструментов.

Коботы могут стать опасными из-за хакерской атаки

Этот миф скорее раздувает сенсацию, чем отражает реальные жизненные ситуации. На самом деле систему безопасности современных коботов невозможно взломать для того, чтобы изменить или отключить встроенные средства обеспечения безопасности, которые ВСЕГДА остаются в активном режиме. В случае несанкционированного подключения и попытки изменить настройки средств безопасности в процессе работы кобота он автоматически останавливается. Чтобы перезапустить его и возобновить работу, необходимо, чтобы кто-либо из сотрудников, способных обнаружить потенциальную атаку, произвел сброс и перезагрузку системы.

Разумеется, определенная степень открытости программного обеспечения коботов должна сохраняться для того, чтобы заказчики могли обновлять систему, настраивать параметры для выполнения тех или иных задач или подсоединять к коботам другие устройства в рамках решений автоматизации. Несмотря на это, коботы в целом не предназначены для подключения к интернету, и если заказчик настаивает на том, чтобы коботы имели онлайн-доступ, то ответственность за безопасность ложится на его ИТ-подразделение. ИКС

Компактный трехфазный ИБП

Компания Schneider Electric расширила линейку трехфазных источников бесперебойного питания среднего ценового сегмента Easy UPS, представив модели Easy UPS 3L мощностью 500 и 600 кВА (400 В) для использования с внешними батареями.

ИБП Easy UPS 3L поддерживают широкий диапазон входного напряжения (323–477 В) и различное количество батарей в батарейном массиве (свинцово-кислотные с регулирующими клапанами). Максимальный входной ток – 899 А. Суммарные гармонические искажения на входе при полной нагрузке не превышают 3%. КНИ выходного напряжения – менее 2% при линейной нагрузке, менее 4% при нелинейной нагрузке. Эффективность достигает 96%. В режиме перегрузки ИБП обеспечивают работу в течение 10 мин при перегрузке 125%, 60 с – при 150%.

Устройства отличаются компактностью (ширина х высота х глубина – 1000 х 1970 х 850 мм), что уменьшает занимаемую площадь, модульной архитектурой (благодаря чему имеют встроенное резервирование N + 1 по силовой части) и возможностью параллельного подключения. Вес – 640 кг. Зарядное устройство обеспечивает подачу до 22% номинальной мощности ИБП на заряд батарей, что позволяет создавать решения с более длительным временем автономной работы.

ИБП Easy UPS 3L рассчитаны на работу при температуре 0–30°С и относительной влажности 0–95% без конденсата и за счет покрытия плат лаком, наличия сменного воздушного фильтра на передней панели и поддержки нагрузок со стартовыми токами способны функционировать в тяжелых условиях. В комплекте с ними поставляются дополнения и аксессуары, облегчающие интеграцию в различные системы диспетчеризации. При покупке опциональной сетевой карты возможны мониторинг и управление устройствами с помощью пакета облачного программного обеспечения EcoStruxure IT.

www.schneider-electric.ru

Оборудование для мониторинга электроснабжения в ЦОДе

Компания Janitza (Германия) сертифицировала для российского рынка новую серию приборов для контроля качества электроэнергии UMG 800.

Головное устройство UMG 801 является устройством сбора и передачи данных, восьмиканальным анализатором электроэнергии и двухканальным монитором дифференциальных токов в пятипроводных системах электроснабжения TN-C-S и TN-S с контролем тока в нейтрали и контуре заземления. Многофидерный учет с количеством каналов измерения тока до 92 можно реализовать с помощью модулей, которые компактно размещаются в одном электрощите (в стандартном модульном DIN-RAIL-конструктиве) или с помощью стандартного кабеля на расстоянии до 100 м.

Характеристики UMG 801:

- возможность непрерывного измерения – 51,2 кГц (1024 точки на период);
- класс точности – 0,2 (для напряжения, тока и мощности);
- выявление искажений в электросети – до 127-й гармоники напряжения;
- контроль дифференциального тока – от 50 мкА;
- измерение тока – 8 каналов/92 канала при подключении модулей расширения.

В устройствах используются стандартные трансформаторы тока 5А. UMG 801 снабжены шлюзом RS-485, двумя портами Ethernet и портом USB. Поддерживаются стандартные протоколы OPC UA, Modbus TCP, IPv4 и IPv6. Управление можно осуществлять через веб-интерфейс. Устройство укомплектовано модулем флеш-памяти объемом 4 Гбайт.

В комплекте поставляется русифицированное ПО Janitza Gridvis для энергоменеджмента и анализа электросетей. ПО позволяет визуализировать данные об энергопотреблении и отчеты о надежности электросети и резервах электрической мощности. Инструментарий для анализа статистики случайных событий помогает прогнозировать устойчивость и в режиме реального времени контролировать резервирование электроснабжения ЦОДа. Энергоменеджмент соответствует ISO 50001, отчеты – стандартам EN50160 (ГОСТ Р 54149-2010) и EN 61000-2-4 (ГОСТ Р 51317.2.4-2000).

www.janitza.pro/umg800

ИТ-шкафы с повышенной нагрузочной способностью

Компания Rittal представила универсальную систему решений в области серверных шкафов и сетевого оборудования на основе обновленной линейки ИТ-шкафов VX IT.

Благодаря улучшенной конструкции рамы ИТ-шкафы имеют большую жесткость 19-дюймового вертикального профиля по сравнению с предыдущей моделью. Шкафы VX IT выпускаются в двух исполнениях. Шкаф VX IT standard выдерживает статическую нагрузку 1500 кг по итогам испытаний в Rittal и 1200 кг по сертификату UL (американская компания по стандартизации и сертификации в области техники безопасности Underwriters Laboratories). Вариант VX IT dynamic допускает нагрузку до 1800 кг согласно испытаниям Rittal и 1500 кг – по сертификату UL. Высота шкафов – от 15 до 52 U.

Монтаж ИТ-шкафа производится преимущественно без инструментов с использованием технологии Snap-In. Маркировка единиц высоты и размеров по глубине позволяет отрегулировать расстояние между 19-дюймовыми плоскостями. Все плоские детали, например боковые стенки и потолочные панели, легко устанавливаются благодаря защелкам и элементам позиционирования. Вертикально разделенные боковые стенки оснащены шарнирами, могут открываться как двери и при этом просто демонтируются. Кроме того, имеются горизонтально разделенные боковые стенки, которые упрощают доступ, например, к серверам.

Для индивидуального монтажа VX IT доступны различные комплектующие: варианты дверей, боковых стенок, основания и крыши, элементы и средства организации кабеля, а также светодиодная рейка для индикации статуса и решения для мониторинга, электропитания и управления оборудованием внутри шкафа. Для внутреннего монтажа VX IT имеются PDU, ИБП, системы ИТ-охлаждения и модули раннего пожарообнаружения и тушения.

Шкафы VX IT испытаны и сертифицированы согласно стандартам UL 2416, МЭК 60950 и МЭК 62368. VX IT совместимы с системами Rittal RiMatrix и другими ИТ-инфраструктурами, которые создаются на базе компонентов Rittal.

www.rittal.ru

Однофазные ИБП с функцией «холодного» старта

Российский разработчик и производитель комплексных решений для защиты электропитания ЦРИ «Импульс» выпустил новую линейку линейно-интерактивных ИБП семейства «Мастер», в которую входят однофазные ИБП мощностью 600–1000 ВА.

ИБП серии «Мастер» предназначены для защиты электропитания ответственной нагрузки. Устройства построены на современной компонентной базе с использованием интеллектуальных микропроцессоров, имеют встроенную панель управления, повышающий/понижающий преобразователь напряжения (AVR), встроенный коммуникационный USB-порт, поддерживают функцию «холодного» старта и автоматического рестарта.

AVR автоматически компенсирует колебания входного напряжения, тем самым минимизируя использование ресурса аккумуляторной батареи, что способствует увеличению продолжительности срока ее службы. Функция «холодного» старта обеспечивает возможность включения ИБП при отсутствии напряжения на его входе.

Эргономичный дизайн устройства предоставляет доступ ко всем разъемам сверху. Встроенная USB-зарядка позволяет заряжать телефон или планшет, подключая их непосредственно к USB-разъему на корпусе ИБП. Наличие интеллектуального USB-порта обеспечивает возможность управлять питанием в режиме реального времени и осуществлять мониторинг статуса ИБП. Имеется встроенная защита при перегрузке и коротком замыкании на выходе устройства, программирование и другие функции управления, а также встроенная функция автовосстановления (авторестарт) подачи питания на нагрузку при появлении напряжения во входной сети.

Диапазон входного напряжения составляет 162–290 В, что позволяет ИБП обеспечивать питание чувствительной нагрузки с минимальным использованием ресурса АКБ.

ИБП «Импульс» серии «Мастер» доступны в версиях со светодиодной индикацией и с ЖК-дисплеем. С помощью встроенных средств индикации отображаются режимы работы ИБП, перегрузка, уровень нагрузки, неисправность, уровень заряда АКБ, а также значения входных и выходных параметров устройства.

www.impuls.energy

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

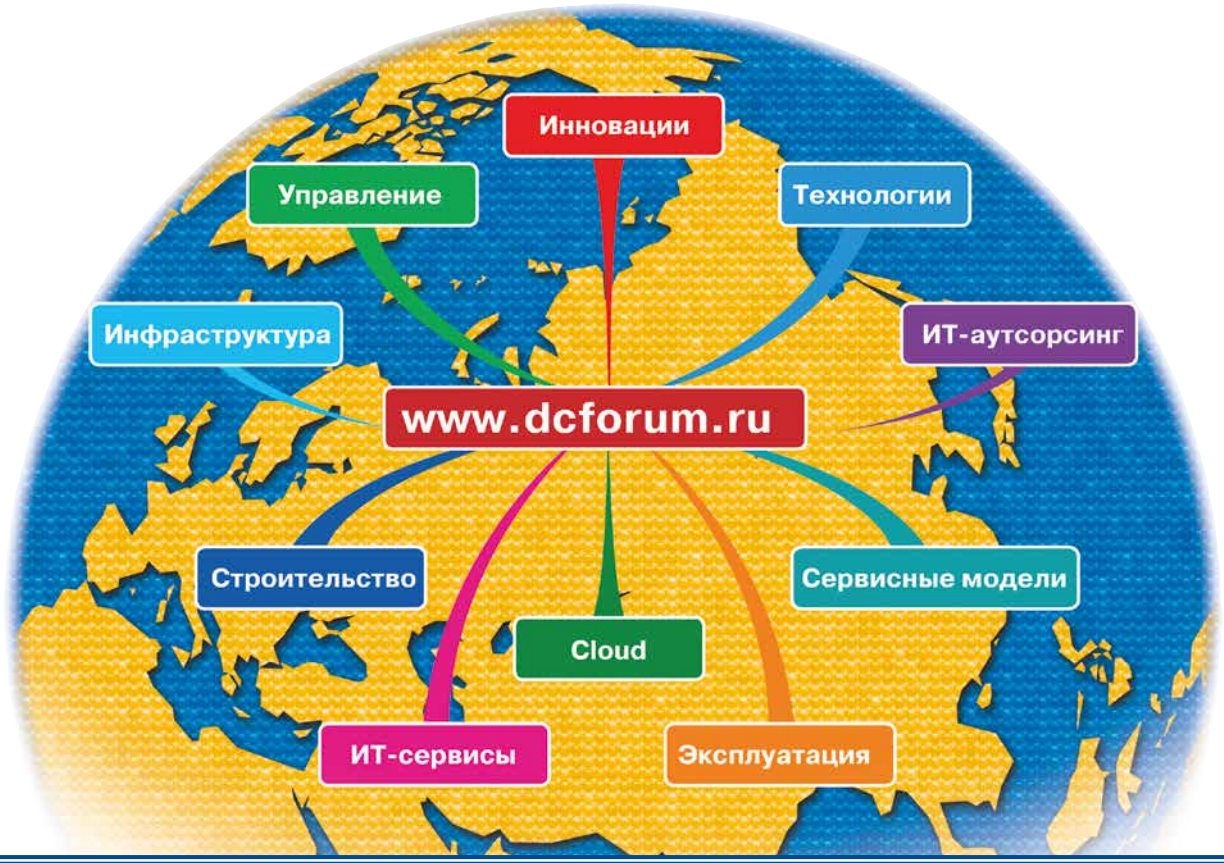
МНТОРЭС им. А.С. Попова:
107031, Москва, ул. Рождественка,
д. 6/9/20, стр. 1;
тел.: (495) 921-1616.

15-я международная конференция и выставка

ЦОД

20 октября 2020
Москва, Holiday Inn Miscow Sokolniki

DATA CENTER FORUM



Реклама 16+

При поддержке

Минкомсвязь России

При участии

Координационный совет по ЦОДам и облачным технологиям
Автономная некоммерческая организация

Uptime Institute

Спонсоры и партнеры

SberCloud · Life Is On Schneider Electric · HUAWEI · RITTAL · 3data Premium Data Centers · IXcellerate · HTS

Check Point Software Technologies Ltd. · VERTIV · Свободные технологии инжиниринг · SME · Группа Компаний Пожтехника · mtu A Rolls-Royce solution · Atos

Allied Telesis · Mitsubishi Electric Changes for the Better · ARISTA · DKC · SUSE · Kelvion · HITEC Power Protection

C3 Solutions Качественно.Сделано.В России. · Акционерное общество Абсолютные технологии · powerconcept Battery Solutions · Импульс Источники бесперебойного питания · Anker Industrial Group · ГрандМоторс Kohler SDMO · GS NANOTECH GS Group

Платформа цифрового развития

| Дата-центры | Облачные сервисы | Услуги связи | Хранение данных

3data
Premium Data Centers

+7 (495) 800-1-800
+7 (800) 505-1-800

dc3data

3data.ru