

ТЕМА НОМЕРА

ГРАНИ РААС

От «серверхоны» к ЦОДам	7	Игры в облаках	80
IX-вектор в эволюции ЦОДов	60	Мой ЦОД – моя крепость	84

ИнформКурьер-Связь

ИКС

издается с 1992 года

Василий Углов

*Технический директор,
Marioff Russia*

Противопожарная защита ЦОДов: мыслить за пределами традиционных решений



2-я международная конференция и выставка

«ЦОД: модели, сервисы, инфраструктура»

28 ноября 2019, Екатеринбург, Hyatt Regency Ekaterinburg

Основные вопросы конференции:

- Аналитика iKS-Consulting. Анализ потребности в дата-центрах и их востребованности в УФО
- Развитие рынка облачных услуг в РФ и регионах
- Мировые тренды в области развития сервисных моделей и инфраструктуры ЦОДов
- Географические, климатические, экономические преимущества развития ЦОДов в УФО
- Современные технологии и решения для инженерной и ИТ-инфраструктуры ЦОДов
- Переход в облако. Конвергентные и гиперконвергентные решения
- Edge и Fog Computing – помощники или конкуренты Облаку?
- Безопасность облачных решений и ЦОДов

При участии



Uptime Institute®



Организатор



www.ekb.dcforum.ru

16+

Реклама

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

Спонсоры и партнеры



Western Digital.



COMMSCOPE®

VERITAS™



Janitza®



ПРЕОРА

УЦСБ

Издается с мая 1992 г.

Издатель
ООО «ИКС-Медиа»участник
АНО КС ЦОДКООРДИНАЦИОННЫЙ СОВЕТ
ПО ЦОДам и ОБЛАЧНЫМ ТЕХНОЛОГИЯМ
Автономная некоммерческая организация

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 – ustionova@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.

Мнения авторов не всегда отражают точку зрения редакции. Статьи с пометкой «бизнес-партнер» публикуются на правах рекламы. За содержание рекламных публикаций и объявлений редакция ответственности не несет. Любое использование материалов журнала допускается только с письменного разрешения редакции и со ссылкой на журнал.

Рукописи не рецензируются и не возвращаются.

© «ИнформКурьер-Связь», 2019

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

реклама

Редакция пользуется
облачными услугами 3data

№4/2019 подписан в печать 01.11.19.

Тираж 8 000 экз. Свободная цена.

Формат 64x84/8

ISSN 0869-7973

12+

ЦОДы и энергетики



ЦОДы зависят от энергетиков. Без подключения к электросетям сегодня не обходится ни один дата-центр. Да и объемы потребляемой ими энергии быстро растут. По уровню энергопотребления все ЦОДы в мире уже сопоставимы с такой огромной страной, как Россия, и существенно опережают менее крупные страны.

ЦОДы тянутся к энергетикам. В поисках надежных и недорогих источников электричества инвесторы начинают строить дата-центры поближе к электростанциям. Хороший пример – крупнейший в России ЦОД в г. Удомля, построенный вблизи Калининской АЭС. Прорабатываются и другие проекты строительства ЦОДов рядом с энергообъектами, например с Няганской ГРЭС в Югре.

Казалось бы, энергетики должны видеть в крупных ИТ-объектах своих ценных клиентов. Должны понимать специфику таких объектов. Но, похоже, это далеко не так.

Когда верстался номер, заключительную стадию согласования проходил подготовленный Минэнерго России проект постановления Правительства РФ, который предусматривает введение оплаты неиспользуемого резерва присоединенной мощности. Эта инициатива может серьезно затронуть многие ЦОДы, которые находятся в процессе развития и еще не вышли на проектные мощности. Она делает бессмысленным применение энергосберегающих технологий, позволяющих снижать энергопотребление в холодное время года за счет фрикулинга. Наконец, ставится под угрозу надежная работа ИТ-комплексов. Для катастрофоустойчивого функционирования такой комплекс разносится минимум по двум удаленным площадкам. При этом нагрузка на обеих будет существенно ниже 100%, чтобы в случае аварии и переброса всей нагрузки на одну из площадок обеспечить ее работу. А в соответствии с инициативой Минэнерго ЦОДам будет невыгодно держать мощности под резерв.

Чем сегодня, когда ИТ становится основой все большего числа бизнес- и производственных процессов, чревата остановка ИТ-сервисов? Серьезнейшими финансовыми потерями, а возможно, и катастрофой с ужасными экологическими последствиями и гибелью людей.

Энергетикам не следует забывать и вот о чем: процессы цифровизации приведут к тому, что они сами будут все сильнее зависеть от ЦОДов, от их современных сервисов хранения, обработки и анализа данных. Ведь данные – это энергия новой экономики.

С надеждой на здравый смысл
и взаимопонимание,
Александр Барсков

Грани РААС

с. 68

1 КОЛОНКА РЕДАКТОРА

4 ИКС-Панорама

- 4 Россия как edge и edge в России
- 7 Узбекистан: от «серверхоны» к ЦОДам
- 10 Питер в ожидании
- 12 ДАЙДЖЕСТ ОТРАСЛИ ЦОДОВ
- 14 Edge: близко, ближе, совсем рядом
- 17 КАЛЕНДАРЬ СОБЫТИЙ

18 Экономика и бизнес

- 18 Т. Толмачева. ВЭФ-2019 как зеркало контрастов Дальнего Востока
- 23 С. Гацакова. Может ли Россия стать крупным поставщиком ПО для целых регионов мира?
- 26 Д. Васюков. Оцифровать урожайность



с. 14

Edge: близко, ближе,
совсем рядом



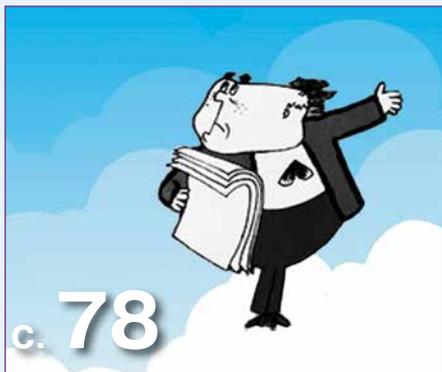
с. 18

Т. Толмачева.
ВЭФ-2019 как зеркало
контрастов Дальнего Востока



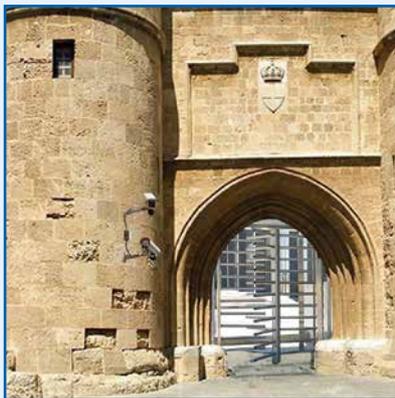
с. 28

А. Эрлих.
Круглогодичный фрикулинг в России, или Готовых рецептов нет



с. 78

С. Зинкевич.
Сценарии использования облачной «песочницы»



с. 84

А. Котов.
Мой ЦОД – моя крепость. Рубежи физической безопасности дата-центра

28 Инфраструктура

- 28 А. Эрлих. Круглогодичный фрикулинг в России, или Готовых рецептов нет
- 33 В. Углов. Пожаротушение в ЦОДе. Откажитесь от штампов
- 36 А. Барсков. PFM задают тренд
- 42 В. Гречушкин. Edge как искусство
- 44 С. Орлов. Системы хранения данных: актуальные тренды
- 48 А. Кюн. Edge-ЦОД Rittal для промышленности
- 50 И. Рундель. Будущее сейчас: технологии ИИ в дата-центрах
- 54 А. Пивоваров. Нейронные сети в глубоком обучении
- 58 Гибридный охладитель JAEGGI – уникальное решение на рынке ЦОДов
- 60 А. Перекрест. IX-вектор в эволюции ЦОДов
- 62 Н. Ефимов. Быстрый, быстрее, самый быстрый: Wi-Fi 6 и кабельные среды
- 65 Д. Рогов. Язык без костей: на чем пишут код современные программисты

68 Сервисы и приложения

- 68 Н. Носов. Грани PaaS
- 75 Н. Носов. Лучше меньше, да лучше
- 78 С. Зинкевич. Сценарии использования облачной «песочницы»
- 80 Н. Носов. Игры в облаках

84 Безопасность

- 84 А. Котов. Мой ЦОД – моя крепость. Рубежи физической безопасности дата-центра
- 89 А. Гавриченко. Утечки трафика: можно ли починить фундамент Глобальной сети
- 92 М. Кондрашин. Контейнерная виртуализация: преимущества и проблемы безопасности

94 Новые продукты



Россия как edge и edge в России

Устранение дисбаланса на глобальном рынке хранения и обработки данных стимулирует развитие дата-центров в России. Но и в самой стране требуется усилить проникновение ЦОДов в регионы в противовес нынешней чрезмерной их концентрации в столице.

Как обеспечить строительство ЦОДов в регионах – один из главных вопросов, обсуждавшихся на организованной «ИКС-Медиа» 14-й международной конференции «ЦОД-2019».

«Мы видим необычайно высокую степень концентрации ИТ-индустрии на рынках США и Юго-Восточной Азии. Большие страны, такие как Бразилия и Россия, находятся на периферии мирового рынка, в edge-регионах», – заявил Гай Вилнер, соучредитель и генеральный директор IXcellerate. В отставании есть свое преимущество – сейчас дисбаланс сглаживается, основной рост идет на новых рынках. «Мы собрались в нужном месте, российский рынок будет развиваться очень быстро. Каждый российский город-миллионник в течение десяти лет будет иметь свой ЦОД», – дал оценку перспектив международный эксперт.

Российский рынок коммерческих ЦОДов растет интенсивно. В 2018 г., по данным iKS-Consulting, он оценивался в 28,5 млрд руб. с годовым ростом в 30%, а в 2019-м достигнет 36,2 млрд руб. Наибольший прирост рынку дают облака – 57% в 2018 г. Как указал директор по развитию бизнеса iKS-Consulting Дмитрий Горкавенко, за последние три года введено в эксплуатацию 34% всех действующих стоек, а по оптимистичному сценарию развития российской экономики в 2024 г. число стоек достигнет 87 тыс.

Лучше всего дела обстоят в Москве, она стремительно становится российским Сингапуром. При декларируемых государством задачах развития регионов доля Москвы на рынке ЦОДов только увеличилась – с 70 до 73%.

При этом большая часть территории страны не может похвастаться нормальным доступом к облачным услугам (рекомендованное для услуг IaaS время отклика – не более 50 мс). В крупных городах Сибири интервал времени между отправкой пакета в московский дата-центр и получением ответа превышает 50 мс, а на Дальнем Востоке уходит за сотню. Решить проблему может строительство там ЦОДов, но для этого государство должно сделать регионы

более привлекательными для бизнеса.

Государство и ЦОД

Ключевой доклад на конференции сделал заместитель министра цифрового развития, связи и массовых коммуникаций РФ Олег Иванов. Рассказывая о ходе реализации федерального проекта «Информационная инфраструктура» нацпрограммы «Цифровая экономика России» и о его влиянии на развитие центров обработки данных, он сообщил, что в настоящее время усилия направлены на обеспечение широкополосного доступа в интернет населения, органов государственной власти и социально значимых объектов (СЗО). К системам беспроводного широкополосного доступа будет подключено 12 980 СЗО в населенных пунктах с численностью жителей сто человек и более. Планируется подключить 370 СЗО в 2020 г. и 12 610 в 2021-м. К ВОЛС подключат 68 038 СЗО: 26% в 2019 г., 32% в 2020 г., 42% в 2021 г.

Рост трафика приведет к увеличению спроса на хранение данных в ЦОДах, да и внедрение сквозных технологий и цифровых платформ для государства, граждан и бизнеса невозможно без сформированного рынка облачных услуг. «Развитие инфраструктуры хранения и обработки данных пока находится в некоей тени. Но надо понимать, что, создав условия для роста системы ЦОДов в регионах и обеспечив взрывной спрос на хранение данных, мы стимулируем рынок к

строительству дата-центров по всей стране», – подчеркнул Олег Иванов.

Основная сложность работы по реализации федерального проекта – отсутствие полных верифицированных данных о сетях





связи и инфраструктурных элементах. Сегодня достоверность этих данных не превышает 70%. До конца года планируется создать Генеральную схему сетей связи и центров обработки данных страны, включающую информацию о существующей инфраструктуре.

Начата подготовка к созданию «тепловой карты» регионов, с целью установления приоритетных субъектов РФ для создания дата-центров, которые позволят удовлетворить потребности в услугах хранения и обработки данных государства, бизнеса и граждан с учетом задач цифровой экономики.

Предполагается, что карта будет содержать конкретные характеристики субъектов РФ, населенных пунктов и площадок для строительства ЦОДов. Она поможет определить целесообразность создания дата-центров в том или ином регионе страны. В рейтинге учитывается деловая активность – количество предприятий в регионе, отраслевая структура и обороты бизнеса, практика использования облачных сервисов и другие параметры. Оценивается и открытость регионов – число технопарков и их резидентов, ИТ-мероприятий и конференций.

Предварительные данные свидетельствуют, что во многих регионах пока нет предпосылок для создания ЦОДов. С другой стороны, наряду с лидерами – Москвой, Санкт-Петербургом, Татарстаном – выглядят привлекательными для строительства ЦОДов и такие неочевидные регионы, как Ханты-Мансийский автономный округ – Югра. «При регулярном обновлении карты мы увидим динамику по регионам, она станет полезным инструментом для государства и бизнеса», – отметил Олег Иванов. Система будет запущена в конце следующего года.

Российский рынок коммерческих ЦОДов мог бы получить мощный толчок к дальнейшему развитию, если бы в них более активно пошли государственные за-

казки. Но здесь серьезным барьером является несовершенство законодательства. «Я еще не видел ни одного инвестора, который согласился бы направить пару миллиардов рублей на создание инфраструктуры с контрактом длительностью максимум два года... Для формирования рынка облачных услуг нужно убрать законодательные барьеры в сфере размещения госзаказов на услуги. Это первоочередная мера, которую надо принять. У нас в плане работ стоит внесение [соответствующих] изменений в законодательство», – отметил директор Департамента развития архитектуры и координации информатизации Министерства цифрового развития, связи и массовых коммуникаций РФ Василий Слышкин.

Edge и megaЦОДы

Задача минимизации передаваемого трафика и уменьшения задержек решается с помощью edge computing, выноса вычислительных мощностей на границу сети. Скажем, Microsoft, Google и Amazon рассматривают свои megaЦОДы в Европе как edge-объекты. Но в России западные гиперскейлеры опасались строить свои дата-центры и в более спокойные годы, а в нынешней политической обстановке такие перспективы выглядят полной фантастикой. Хорошо, что еще есть IXcellerate, которая активно вкладывается в российский рынок colocation и после ожидаемого поглощения «Ростелекомом» компании DataLine займет второе место на нашем рынке.

Более вероятна экспансия с рынка Юго-Восточной Азии, прежде всего из Китая. В Москве уже обжилась Huawei, подтягиваются Alibaba и China Telecom. Если китайский бизнес активно пойдет в российские регионы, то ему понадобится и привычная ИТ-инфраструктура. Так что можно ожидать участия восточного соседа в строительстве ЦОДов в регионах страны, переноса его вычислительных мощностей все дальше в Россию на границы своих расширяющихся сетей, тем более что Китай обладает необходимыми для этого ресурсами. Взять хотя бы упомянутую Huawei, которая производит всю линейку оборудования для ЦОДов, включая инженерные реше-





ния, сетевое и вычислительное оборудование, что, по словам старшего менеджера Huawei по решениям ЦОД Артура Хашимова, позволяет создавать из них комплексные решения с оптимальным энергопотреблением.

Вендоры ждут

Наибольшие надежды связываются с российскими игроками, которые, насытив рынок столицы, должны пойти в регионы. Особенно если государство снимет законодательные барьеры, а еще лучше – стимулирует строительство новых ЦОДов. Нужна активная поддержка сверху нового «цифрового ГОЭЛРО». Роль крупных гидроэлектростанций будут играть большие ЦОДы, более мелких – мини-ЦОДы, электроразделов небольших предприятий – микро- и наноЦОДы (меньше стойки). Эти разные по величине точки передачи и обработки трафика станут важнейшими элементами цифровой трансформации, объединяя ИТ-инфраструктуры предприятий в единое цифровое пространство.

ЦОД расширяет свои границы на периферийные устройства. «Но периферийные устройства, которые являются не менее критичной частью инфраструктуры, зачастую формируются по остаточному принципу», – отметил вице-президент подразделения Secure Power Schneider Electric в России и СНГ Роман Шмаков, подчеркнув, что общая надежность и доступность систем определяется самым узким местом. Необходимо стандартизировать периферийные устройства, делать их легкими для развертывания и подключения к общей инфраструктуре. Для этого целесообразно использовать решения высокой заводской готовности (prefabricated), при необходимости адаптируя их к конкретным нуждам заказчика. Эксперт выделил три области периферийных вычислений: торговые предприятия и офисные пространства с уклоном на обработку данных пользователей; телеком, где основной фокус – на надежности и качестве передачи данных; промышленные предприятия с автономными устройствами, имеющими «умную» составляющую.

Edge-ЦОДы «из коробки» важны для Индустрии 4.0, когда сеть edge-устройств предприятия обрабатывает и передает данные в облако. При этом, как указал ведущий менеджер компании Rittal Кирилл Дмитриев, имея дело со старыми производственными зданиями, надо учитывать снижение несущей способности их перекрытий. Компактные решения Rittal вписываются в нагрузку око-

ло 400 кг/ кв. м, что значительно ниже стандартной несущей способности перекрытий административных зданий (700 кг/кв. м). При наличии всех необходимых инженерных систем в шкафу остается не менее 60% пространства для активного оборудования.

Чем больше становится данных, тем актуальнее вопрос их хранения. Директор по продажам израильской компании Infinidat Алексей Капранов рассказал, что система хранения InfiniBox может обеспечить емкость до 4,1 Пбайт в одном шкафу 42U при скорости 2 млн IOPS (более 95% операций выполняется в кэше) и высокой доступности (анонсированная надежность – семь девяток). Израиль не участвует в санкционных войнах с Россией, что тоже может иметь значение для отечественных заказчиков.

Надежнее и быстрее

На наших глазах создается новый цифровой мир. Виртуальная реальность, потоковое видео, игры – огромные объемы данных выдвигают новые требования к их передаче, в том числе в ЦОДах. По словам технического менеджера ERA компании Siemon Ли Фаннела, в ближайшие пять лет в мире будет потрачено \$25 млрд на трансформацию дата-центров. Он призвал не ориентироваться на стандартные кабели категории 6 при проектировании новых ЦОДов, а использовать новые высокоскоростные каналы коммуникации.

Для обеспечения доступа к облачным сервисам и трансформации регионального бизнеса на огромной территории страны понадобятся надежные каналы связи между edge- и основными ЦОДа. Помочь может технология SD-WAN. Решение такого класса предлагает, в частности, компания Citrix. Как рассказал главный инженер Citrix Сергей Халяпин, из разных каналов (спутник, интернет, MPLS) создается виртуальный «умный» и безопасный канал между устройствами SD-WAN. При этом они направляют трафик по наилучшему пути в зависимости от состояния конкретных каналов. Каждый поток может направляться со своим приоритетом в зависимости от приложения и переключаться на другой канал при возникновении проблем.

...Конференция прошла в атмосфере оптимизма – рынок российских ЦОДов на подъеме, работы много, места на рынке хватит для всех.

Николай Носов

Узбекистан: от «серверхоны» к ЦОДам



Низкая стартовая база, наличие стандарта, доступность самых современных технологий и очевидный тренд к цифровизации – хорошие условия для быстрого развития рынка дата-центров Узбекистана. Но нужны инвесторы, которые поверят в этот рынок.



Проведенная «ИКС-Медиа» в начале октября первая международная конференция и выставка «ЦОД: экономика, инфраструктура, сервисы» стала важным событием для ИКТ-рынка Узбекистана. По сути первый профессиональный форум такого уровня в стране должен послужить толчком, который ускорит развитие рынка центров обработки данных и облачных сервисов.

Вчера

Примерно до середины 2010-х гг. в Узбекистане существовали лишь серверные комнаты, по-узбекски – «серверхона». Причем, по словам Улугбека Каланова, генерального директора компании Integracia, учитывая их состояние, букву «о» в слове «хона» вполне можно было заменить на «а». В такие недоЦОДы принимали на colocation все что угодно, любые, в том числе самосборные, серверы, при том что рядом мог стоять серверный комплекс от именитого бренда стоимостью полмиллиона долларов. Пожар мог возникнуть из-за такой самосборки, а пострадать – клиент с серьезной системой, критически важной для его бизнеса.

Инженерное оборудование типичной «серверхоны» оставляло желать много лучшего. «Какое-то энергообеспечение – хорошо если первой категории, но без батарей для резервирования; какое-то кондиционирование – начиналось все со знаменитых бакинских кондиционеров; какое-то пожаротушение – бытовые огнетушители; какой-то контроль доступа – заходи кто хочешь, делай что хочешь», –

вспоминал У. Каланов. Приятное исключение составляли ЦОДы операторов связи с международным опытом, в частности МТС и «Вымпелкома». Но такие объекты они строили для себя и как коммерческие не использовали.

ИКТ-объекты начали приводиться в порядок в 2013–14 гг. Важной вехой стало создание в 2013 г. Центра технического содействия – государственной инспекции по контролю в сфере информатизации и телекоммуникаций, где были собраны специалисты с высоким уровнем экспертизы по всем направлениям ИКТ. В 2014 г. в Узбекистане был принят в качестве ГОСТа государственный стандарт, определяющий требования к дата-центрам. Документ был разработан специалистами «Узинфокома» (единственный интегратор, занимающийся созданием и поддержкой государственных информационных систем) при содействии экспертов ЦТС.

Примерно тогда же начали строиться коммерческие ЦОДы для предоставления услуг по модели В2В. Первая ласточка – дата-центр уже упомянутого «Узинфокома» (на сегодня порядка 20 стоек). Затем был построен коммерческий ЦОД «Узбектелекома», вслед за ним – дата-центр в ташкентском Университете Инха. Есть и по меньшей мере один ЦОД, «заточенный» под облачные сервисы, – его развернула компания «Вымпелком». Но общую емкость коммерческих ЦОДов в Узбекистане аналитики iKS-Consulting оценивают в 80–100 стоек.

Наверное, самым крупным ЦОДом в Узбекистане является объект «Узбектелеко-





ма» – модульный контейнерный дата-центр, построенный за пределами Ташкента. Он примерно в 100 раз меньше самого крупного ЦОДа в России (в Удомле), хотя и тот по емкости значительно уступает зарубежным гипер-ЦОДам. Понятно, что перспективы роста огромны. А есть ли рынок?

Сегодня

Найти сейчас в Узбекистане место в качественном надежном коммерческом ЦОДе – задача непростая. «За последние пять лет я обошел практически все коммерческие площадки в стране с одной целью: встать на colocation. И каждый раз обнаруживал критические минусы, которые помешали бы работе моего сервиса. Самая главная проблема – энергоснабжение. В одном из ЦОДов простой пять часов в месяц мне объяснили просто: “У нас не было света”», – пожаловался У. Каланов.

Налицо – дефицит предложения. Неудивительно, что узбекские компании предпочитают размещать свои ИТ-оборудование и сервисы на собственных площадках, уровень которых за последние пять лет существенно вырос. Но этот подход противоречит мировому тренду, согласно которому все больше заказчиков выбирают сервисную модель и используют услуги коммерческих ЦОДов.

Как отметил, выступая в Ташкенте, Дмитрий Горкавенко, директор по развитию бизнеса iKS-Consulting, в мире доля стоек, размещенных в коммерческих ЦОДах или у облачных провайдеров, динамично растет. На сегодня она составляет порядка 40%, но уже к 2024 г. превысит 50%. Однако, скажем, в России этот показатель всего 14%. Что же касается ряда стран СНГ, то применительно к ним вообще рано говорить о становлении рынка коммерческих ЦОДов как такового. Это относится и к Узбекистану.

По мнению аналитика iKS-Consulting, хорошей основой развития цифровой инфраструктуры Узбекистана является человеческий капитал – в стране много образованных людей, грамотных специалистов. А вот слабое развитие инфраструктуры – серьезный сдерживающий фактор. По данным ERGO Research & Advisory, около 17,2 млн (53%) населения Узбекистана

испытывают проблемы с использованием сотовой связи из-за некачественного покрытия. Многие не выходят в интернет из-за недоступности и/или недостатка цифровых навыков либо отсутствия цифрового контента. В Узбекистане проложено около 24,5 тыс. км оптоволоконных линий, что немного для страны такого размера. Наконец, Узбекистан сильно зависит от международных наземных магистральных каналов для передачи данных. Удаленность от Мирового океана ограничивает доступ к магистральным подводным линиям.

Инфраструктурные проблемы подтверждают и местные специалисты. Бахтиер Умаров, генеральный директор Tosh Temir Savdo, выделил три проблемы, тормозящие процессы строительства ЦОДов в Узбекистане. Две из них обусловлены ситуацией на телекоммуникационном рынке: это «слабый» интернет и сложности с подведением к ИКТ-объектам волоконно-оптических каналов из-за государственной монополии на соответствующие ресурсы. Третья связана с существующими инженерными коммуникациями – они затрудняют обеспечение соответствия высоким требованиям отказоустойчивости, например Tier III.

Да и опыта специалистам, работающим в Узбекистане, еще явно не хватает. Взять, например, ЦОД Университета Инха – один из самых современных в стране. Все сделано правильно и красиво, однако при расчетах специалисты исходили из среднегодового уровня вод. Но когда весной нынешнего года в Ташкенте прошли сильные дожди, как рассказал У. Каланов, залило и энергетический остров дата-центра, что вызвало простой из-за отключения энергоснабжения. «Нужно учитывать, что иногда случается форс-мажор. Если бы строители сделали подушку на полметра выше, ничего бы не случилось», – отметил он.

Собственно, и в России ЦОДостроители в свое время тоже набили немало шишек. «У нас было сделано много технологических ошибок на очень хороших площадках. В итоге эти площадки так и не раскрыли того огромного потенциала, который был в них изначально заложен», – поделился

опытом Александр Мартынюк, генеральный директор «Ди Си квадрат».

Обращаясь к делегатам конференции, он сказал: «У вас большое преимущество. Вы имеете возможность не совершать все те ошибки, которые я наблюдал последние 15 лет на рынке России. Вы можете воспользоваться результатами огромной работы, которая была проведена специалистами в соседних странах, и внедрить их у себя. У вас нет никаких препятствий с точки зрения технологий и оборудования, вам доступны самые передовые решения мировых лидеров».

Следует отметить, что поставщики таких решений проявляют все больший интерес к узбекскому рынку. На форуме в Ташкенте свои комплексные решения для организации инженерной инфраструктуры ЦОДов представили Schneider Electric и Tripp Lite. Большой интерес делегатов вызвали системы на базе динамических ИБП, о которых рассказали специалисты Hites и «ГрандМоторс». Свои серверные решения презентовала компания Atos – при спаде маркетинговой активности ИТ-грандов она явно рассчитывает «снять сливки» на хоть и небольших, но быстрорастущих рынках, таких как узбекский.

Все более востребованными становятся и небольшие полностью укомплектованные дата-центры (микро-, мини-ЦОДы), и модульные решения, позволяющие сократить сроки создания ИКТ-комплексов. Подобные решения производят не только мировые игроки, такие как уже упоминавшаяся Schneider Electric, но и российские компании, которые выходят на рынки стран СНГ. Для Узбекистана свои продукты анонсировали эксперты ДАТАРК, С3 Solutions и GreenMDC. А важные для любого критического объекта средства пожаротушения продемонстрировала компания «Холдинг ОСК групп».

Завтра

Согласно прогнозу iKS-Consulting, основанному на данных ERGO Research & Advisory, в период 2017–2021 гг. среднегодовой рост рынка ИКТ Узбекистана составит 12,9%. При этом, отметил Д. Горкавенко, развитие рынка сервисов пойдет существенно быстрее (CAGR = 22,1%), чем рынка оборудования (12,1%). Сервисная модель будет становиться все популярнее, а значит, существенно увеличится спрос на услуги коммерческих ЦОДов.

Анализируя пути развития рынка ЦОДов Узбекистана, У. Каланов обрисовал три возможных сценария. Первый (эксперт назвал его белорусской моделью) – активное строительство государственных дата-центров: «Государство „говорит“ как своим структурам, так и другим компаниям: не стройте свои маленькие дата-центрики, я сделаю один для всех. Если такой проект успешно реализуется, то он становится драйвером для развития всей ИТ-индустрии, и Беларусь тут хороший пример».

Другой подход – частные, независимые ЦОДы. Так, в Казахстане активный предприниматель Тахир Такабаев на свои и привлеченные средства уже построил коммерческие ЦОДы общей емкостью более 70 стоек – почти как весь рынок коммерческих дата-центров Узбекистана. Его клиентами

являются, в частности, банки, которые размещают в них свои критические ИТ-системы. «Бизнесмен всегда сделает лучше, чем банк или государство. Это очень интересный пример для Узбекистана», – полагает У. Каланов.

Наконец, третий сценарий – государственно-частное партнерство, когда «государство дает то, что оно может дать, а предприниматели берут то, что они хотят взять».

А «дать» государство может, например, площади, освобождаемые на АТС. «Эти здания идеально подходят для ЦОДов. Но их надо грамотно оборудовать», – признал генеральный директор Integracia.

Заметим, что в России в свое время тоже были задумки использовать осво-

бождающие здания АТС. Однако, по словам А. Мартынюка, который обследовал такие здания, далеко не все они подходят для дата-центров. Даже если само здание пригодно для ЦОДа, зачастую отсутствуют необходимые внешние площади для размещения габаритных инженерных систем, например, дизель-генераторных установок и чиллеров.

Но выбор помещений для организации ЦОДа или площадки для его строительства – это уже вопрос технический. Гораздо важнее для Узбекистана найти инвестора, который должен быть в хорошем смысле этого слова авантюристом, чтобы поверить в перспективы рынка. Этим инвестором может выступить государство, заинтересованное в создании платформы для цифровой экономики. Возможно, рынком Узбекистана заинтересуются зарубежные инвесторы, скажем, из Китая, с Ближнего Востока или даже из России, которых привлечет географическое положение Узбекистана для формирования цифрового Шелкового пути.

Основные драйверы, которые должны привести к росту рынка ЦОДов Узбекистана, – это развитие электронного правительства, цифровизация государственного образования, энергетики и ЖКХ, реализация новых методов в добыче полезных ископаемых, в первую очередь газа, и т.д. Все большие объемы данных будут формироваться в результате внедрения цифровых технологий в образование, системы дистанционного обучения, телемедицины, цифрового банкинга. И уровень качества ЦОДов, которого реально достичь в Узбекистане сегодня, может быть гораздо выше того, с которого рынок дата-центров начинал развиваться в России 12–15 лет назад.

**Александр Барсков,
Ташкент – Москва**



Питер в ожидании

Разрыв в темпах роста между московским и петербургским рынками коммерческих ЦОДов за последние два года увеличился. Но ряд предпосылок позволяет прогнозировать переход рынка коммерческих дата-центров Санкт-Петербурга в стадию активного развития.

Прошедшая в Санкт-Петербурге третья ежегодная конференция «ЦОД: модели, сервисы, инфраструктура», организованная «ИКС-Медиа», выявила существенный потенциал рынка коммерческих дата-центров Северо-Западного федерального округа. Его раскрытию должны помочь как интерес к этому рынку со стороны московских игроков, которые могут стать инвесторами ЦОДов СЗФО, так и рост востребованности услуг коммерческих дата-центров у все более широкого круга заказчиков.

По предварительным данным iKS-Consulting, общий рост российского рынка коммерческих ЦОДов в 2019 г. составит 11%, или порядка 4400 стоек. Основной вклад в увеличение числа стоек внесут компании IXcellerate, DataPro, «Ростелеком-ЦОД» и 3data. Трое из этих четырех игроков базируются в Москве. Активизация московских игроков связана с дефицитом свободных площадей в столице и высоким спросом на услуги коммерческих ЦОДов. Именно этот дефицит привел к инициации в 2018 г. ряда крупных проектов, завершение которых увеличит общий показатель роста рынка по всей стране до 25% в 2020 г.

В Санкт-Петербурге ситуация иная. По словам Станислава Мирина, ведущего консультанта iKS-Consulting, свободных ресурсов в городе еще достаточно, поэтому питерские площадки не вошли в число наиболее быстрорастущих. Более того, доля Северной столицы на российском рынке дата-центров постепенно сокращается. Если в 2017 г. на петербургские ЦОДы приходилось 14% рынка (на Москву – 68%), то в текущем году их доля сократится до 12% (Москва – 72%). Но Санкт-Петербург характеризуется высокой концентрацией квалифицированных кадров, а СЗФО имеет высокую долю в ключевых

отраслях российской промышленности. Эти факторы, по мнению эксперта iKS-Consulting, «рано или поздно приведут к тому, что местный рынок перейдет в фазу активного развития».

Коммерческий ЦОД: не дешево, но надежнее

Усиление интереса к сервисной модели служит важным стимулом развития отрасли коммерческих ЦОДов. Практическим опытом переезда в такой дата-центр поделился с делегатами конференции Андрей Пономарев, архитектор ИТ-инфраструктуры компании «Балтийский лизинг». До недавнего времени эта компания с объемом лизингового капитала порядка 50 млрд руб. эксплуатировала собственный ЦОД. Объект был оборудован всеми основными инженерными системами с резервированием. Однако, признал А. Пономарев, «чем сложнее инженерная инфраструктура, тем больше времени и сил требуется на ее обслуживание, да и аварий избежать не удавалось». На обслуживание инженерных систем уходило все больше времени сотрудников ИТ-подразделения. Главным же триггером перехода в коммерческий ЦОД стал отказ бизнес-центра, в котором находился офис компании, продлить договор аренды.

Компания рассматривала семь коммерческих ЦОДов, расположенных в Санкт-Петербурге. Был составлен внушительный перечень требований, касающихся владельца здания, в котором находится ЦОД, наличия и характеристик основных инженерных систем. А. Пономарев обратил внимание на важность расположения площадки, удобства подъезда и парковки автомобиля, комфортной работы в ЦОДе инженеров и сетевых администраторов заказчика. «Если в час пик машину можно поставить только за полкилометра от ЦОДа, это очень неудобно», – сказал он.

В шорт-лист попали три лидера рынка коммерческих ЦОДов Санкт-Петербурга: Selectel,





Xelent, Linxdatacenter, а выбор в результате был сделан в пользу Linxdatacenter. А. Пономарев отметил нюансы самого переезда в коммерческий ЦОД. Так, предложенные расценки на транспортировку ИТ-оборудования первоначально были «несоизмеримы с объемом работ». «Нам удалось сбить эту цену почти в пять раз», – добавил он.

В целом «Балтийский лизинг» доволен выбором, сделанным в пользу размещения ИТ-инфраструктуры в коммерческом ЦОДе. «Мы стали заниматься своими профильными делами, не отвлекаясь на вопросы, связанные с инженерной инфраструктурой. Дешевле не будет, но будет проще, надежнее и увереннее», – подвел итоги перехода к сервисной модели А. Пономарев.

И снова edge

Вот уже на нескольких форумах, проводимых «ИКС-Медиа» в разных городах России и СНГ, тема периферийных вычислений (edge computing) становится одной из ключевых. В Санкт-Петербурге она рассматривалась в первую очередь применительно к развитию дата-центров в регионах России.

Ярослав Городецкий, генеральный директор CDNvideo, выделил три ключевые предпосылки развития edge computing в России. Во-первых, это огромная территория страны и, как следствие, большие сетевые задержки при доступе к облачным ресурсам, находящимся преимущественно в Москве. Во-вторых, высокий уровень проникновения интернета в регионах (доступ к Сети имеет более 75% населения). Наконец, в-третьих, рост числа приложений, требующих минимальной сетевой задержки. «Грядут сети 5G, а с ними и новый класс приложений, для которых задержка до централизованного облака делается критичной», – подчеркнул эксперт.

Увеличению потребности регионов в ЦОДах будет способствовать реализация в стране масштабного проекта подключения социально значимых объектов (СЗО): школ, фельдшерско-акушерских пунктов, органов государственной власти, объектов МВД, МЧС, Росгвардии, ЦИК. Как рассказал Игорь Семенихин, директор департамента инфраструктурных проектов Минкомсвязи России, всего планируется подключить более 80 тыс. СЗО, причем большая их часть (около 68 тыс.) будет подключена по ВОЛС. Генерируемые этими объектами данные потребуют новых современных центров их хранения и обработки, причем не в Москве, а непосредственно в регионах размещения СЗО.

Для выявления регионов, где наиболее целесообразно строить ЦОДы, сейчас создается «тепловая карта» России (подробнее – в статье «Россия как edge и edge в России»). Параллельно с разработкой «тепловой карты» эксперты iKS-Consulting и CDNvideo ведут работу по определению оптимальных мест строительства ЦОДов

для улучшения облачной связности регионов. Текущая ситуация с концентрацией облачных сервисов в Москве и Санкт-Петербурге приводит к недопустимому для многих приложений времени задержки в большинстве регионов страны.

Основываясь на данных о задержках, измеренных на сети CDNvideo, эксперты разработали два варианта размещения дата-центров, при реализации которых для 90% пользователей в России задержка доступа к облачным сервисам не будет превышать 15 мс. Эти конфигурации предполагают развертывание ЦОДов минимум в 17 городах страны.

При построении новых ЦОДов, очевидно, не обойтись без современных технических решений. И производители самым активным образом продвигают такие системы. Например, Rittal делает ставку на возможность развертывания edge-ЦОДов в неподготовленных помещениях. Как отметил Кирилл Дмитриев, ведущий менеджер по продукции «Системы контроля микроклимата» Rittal, даже в решениях на одну стойку при наличии всех необходимых инженерных компонентов до 75% места может быть выделено под полезную нагрузку (ИТ-оборудование).

Компания Schneider Electric представила делегатам конференции в Санкт-Петербурге новинку: edge-ЦОД размером всего 6U. Это решение оснащено всеми необходимыми инженерными системами, что обеспечивает высокий уровень надежности. «Инженерка» занимает 3U, оставляя еще 3U для размещения ИТ-оборудования. При стекировании нескольких конструктивов доля полезного пространства увеличивается. Этот микроЦОД может быть смонтирован на стену или установлен на полу, а наличие колесиков упрощает его перемещение.

В целом в России есть все предпосылки для ускорения темпов роста отрасли ЦОДов: объемы данных стремительно растут, государство оказывает отрасли поддержку и, несмотря на санкции, ей доступны самые современные технологии. Процесс серьезно сдерживает централизация всего бизнеса и деловой активности в Москве. Здоровая децентрализация, а также коррекция приоритетов в направлениях инвестиций смогут стимулировать и развитие рынка Санкт-Петербурга.

**Александр Барсков,
Санкт-Петербург – Москва**



НОВОСТИ АНО КС ЦОД

ИЮНЬ 2019. Регистрация АНО КС ЦОД

13 июня 2019 г. Министерством юстиции РФ было принято окончательное положительное решение о регистрации АНО «Координационный совет по ЦОДам и облачным технологиям».

ИЮЛЬ 2019. Большие парламентские слушания по цифровой экономике

Представители АНО КС ЦОД приняли участие в парламентских слушаниях в Государственной Думе, где обсуждались вопросы создания эффективной правовой базы для цифрового развития страны. Результатом кулуарного общения стало представление АНО КС ЦОД законодателям, представителям правительства и бизнеса, а также обсуждение перспектив принятия государственных мер поддержки отрасли в рамках реализации госпрограммы «Цифровая экономика РФ».

АВГУСТ 2019. Заседание рабочей группы АНО КС ЦОД по популяризации и продвижению сервисной модели и услуг ЦОДов

На встрече обсуждались механизмы присутствия АНО КС ЦОД в СМИ, участие организации в отраслевых мероприятиях. Было принято решение о публикации ежеквартального дайджеста ключевых событий индустрии в журнале «ИКС», а также создание Telegram-канала с отраслевыми материалами различных СМИ. Участники заседания высказались в пользу целесообразности участия АНО КС ЦОД в конференциях «ЦОД» в Москве, Санкт-Петербурге и Екатеринбурге, а также в крупных инвестиционных форумах, таких как ВЭФ, РИФ, СПЭФ.

СЕНТЯБРЬ 2019. Сессия по развитию отрасли дата-центров на ВЭФ 2019 во Владивостоке

Подготовка сессии «Инфраструктура для экономики данных: новые возможности для сотрудничества между Дальним Востоком и АТР» была проведена АНО КС ЦОД совместно с Минкомсвязью России. Модератор сессии, партнер iKS Consulting Татьяна Толмачева от лица отраслевого сообщества и АНО КС ЦОД рассказала о том, как бизнес видит потенциал российского рынка ЦОДов и какие меры предлагает для его реализации. Она, в частности, отметила, что игроки рынка поддерживают все инициативы Минкомсвязи, направленные на стимулирование строительства дата-центров.
Подробности – на с. 13.

СЕНТЯБРЬ 2019. Выступление генерального директора АНО КС ЦОД на «ЦОД-2019»

На пленарной сессии 14-й международной конференции «ЦОД» в Москве Дмитрий Бедердинов рассказал о том, что эксперты АНО активно участвовали в разработке предложений по господдержке отрасли, внесли замечания и предложения в техническое задание на создание Генеральной схемы развития сетей связи и инфраструктуры хранения и обработки данных, сформировали перечень предложений в регламент правил отпуска электроэнергии ЦОДам на оптовом и розничном рынках и т.д. Руководитель АНО КС ЦОД призвал к выработке единой позиции участников рынка по важным для отрасли вопросам и активному взаимодействию с государством.

СЕНТЯБРЬ 2019. Очередное заседание Совета АНО КС ЦОД

На заседании, которое прошло в рамках конференции «ЦОД» в Москве, был рассмотрен ряд вопросов, касающихся организационной деятельности АНО КС ЦОД. Состав учредителей АНО пополнился еще одной организацией – АО «КОНСИСТ-ОС», дочерней структурой концерна «Росэнергоатом». В рамках встречи обсуждались вопросы, связанные с участием представителей АНО в крупных бизнес-форумах и ближайших отраслевых мероприятиях, взаимодействие с отраслевым министерством, перспективы развития регионального рынка облачных услуг и услуг ЦОДов, а также предлагаемые меры господдержки отрасли ЦОДов.

ОКТАБРЬ 2019. АНО КС ЦОД в Ташкенте

При участии АНО КС ЦОД прошла первая международная конференция и выставка «ЦОД: экономика, инфраструктура, сервисы» в Узбекистане. На форуме выступил член Совета АНО Дмитрий Горкавенко. Как отмечали многие эксперты, по сути первый профессиональный форум такого уровня в стране должен стать толчком для ускорения развития рынка центров обработки данных и облачных сервисов.
Подробности – на с. 7.

ОКТАБРЬ 2019. Конференция в Санкт-Петербурге

АНО КС ЦОД приняла участие в конференции «ЦОД: модели, сервисы, инфраструктура» в Санкт-Петербурге.
Подробности – на с. 10.

НОВОСТИ ОТРАСЛИ

Минкомсвязь разработает рейтинг привлекательности регионов для строительства ЦОДов



Министерство создаст «тепловую карту регионов», отражающую их привлекательность для строительства ЦОДов. Об этом заявил замглавы Минкомсвязи России Олег Иванов. «Система будет запущена к концу 2020 г.», – уточнил замминистра, выступая с ключевым докладом на пленарном заседании 14-й международной конференции «ЦОД». А уже до конца 2019-го планируется утвердить Генеральную схему развития сетей связи и инфраструктуры хранения и обработки данных РФ до 2024 г., напомнил О. Иванов.

Крупнейший в Европе цифровой мегакомплекс планируют построить в Московской области



Фото: istradigital.com

Мегакомплекс ISTRADIGITAL планируется построить до 2024 г. в Истринском районе Московской области на участке площадью 241,5 га. Комплекс будет включать в себя парк центров обработки данных мощностью в 40 тыс. стоек, технопарк (форсайт-центр, научно-исследовательские лаборатории, бизнес-центр, конгресс-холл, кампус, медицинский кластер, гостиничный и спортивный комплексы) и современный агрокластер площадью 120 га.



НОВОСТИ ОТРАСЛИ

Дата-центры готовят региональную экспансию
Московская сеть дата-центров 3data начнет выход в регионы России. Компания планирует работать по модели франшизы и в течение 10 лет открыть до 200 ЦОДов по всей стране. В Москве у 3data более 10 площадок, число которых в течение этого же срока планируется увеличить до 50. Объем собственных инвестиций в развитие компания не раскрывает.

IXcellerate открывает второй дата-центр в России



Компания объявила о завершении строительства и открытии Moscow Two – своего второго дата-центра в России. С вводом в эксплуатацию новых мощностей суммарное количество стойко-мест IXcellerate составило 3315 единиц. ЦОД IXcellerate Moscow Two построен в рекордные сроки – за шесть месяцев. К моменту его открытия текущими и новыми клиентами зарезервировано более 85% мощностей.

DataLine продолжит расширять сеть своих дата-центров

В марте 2020 г. на площадке на Коровинском шоссе планируется запустить ЦОД NORD-5 мощностью 580 стоек. В январе 2021 г. там же заработает NORD-6 мощностью 470 стоек. Дата-центры будут сертифицированы по стандартам Uptime Institute: Design, Facility и Operational Sustainability.



ТАТЬЯНА ТОЛМАЧЕВА
партнер, iKS-Consulting

**АНАЛИТИЧЕСКИЕ РАЗМЫШЛЕНИЯ
О НЕОБХОДИМОСТИ РЕАЛИЗАЦИИ ПОТЕНЦИАЛА
РОССИЙСКОГО РЫНКА УСЛУГ ЦОДОВ**

По оценкам iKS-Consulting, в 2019 г. объем российского рынка услуг центров обработки и хранения данных достигнет 36,2 млрд рублей (\$557 млн в долларовом эквиваленте). Это значительно меньше, чем в странах, сопоставимых с Россией по ключевым социально-экономическим и территориальным характеристикам. В то же время очевидно, что потенциал российского рынка коммерческих ЦОДов значительно выше своего текущего объема.

По нашему мнению, ключевая причина такой ситуации – преобладание модели «собственный ЦОД» как среди корпораций, так и среди компаний государственного сектора. Это сдерживает спрос на инфраструктуру и существенно влияет на сроки утилизации стойко-мест, а значит, и на сроки ввоза инвестиций.

На коммерческие ЦОДы приходится около 10% общего числа установленных в России стоек. Остальные принадлежат среднему и крупному бизнесу (86%) и организациям государственного сектора (примерно 4%). Такая структура не позволяет создать оптимальную с точки зрения использования эффекта масштаба и географического распределения сеть ЦОДов в РФ. В результате дата-центры размещены по территории нашей страны крайне неравномерно, а цены на их услуги растут.

В настоящее время общий уровень цифровой зрелости российского бизнеса довольно низок. Отдельные элементы цифровой платформы хотя и внедряются, но в большинстве случаев не взаимосвязаны. Внедрение цифровых технологий носит фрагментарный характер. Общий уровень зрелости ключевых процессов недостаточен для модификации бизнес-модели с помощью цифровых технологий.

Именно поэтому мы считаем, что сегодня критически важно мягко подталкивать бизнес к тому, чтобы он оцифровывал свои данные, переводил документооборот в электронный вид, цифровизировал максимальное количество рабочих процессов сквозным образом.

А значит, необходимо продолжать применять меры экономического и администра-

тивного воздействия для дальнейшего перевода бизнеса в цифровой вид, вводить обязательные режимы электронного взаимодействия с бизнесом и обмена данными в цифровом виде.

Положительный опыт побуждения бизнеса к переходу на электронный документооборот уже есть. Например, сделана обязательной сдача налоговой и иной отчетности в контролирующие органы по каналам электронного взаимодействия через операторов электронного документооборота, введены онлайн-кассы в розничной торговле и др.

Очевидно, что реализация национальных проектов, ориентированных на развитие цифровой экономики, обеспечит гарантированный спрос со стороны государства и бизнеса на услуги коммерческих центров обработки и хранения данных, облачных сервисов. По нашим оценкам, на разработку информационно-сервисных и информационно-аналитических систем и платформ для государственного сектора по национальным проектам «Цифровой экономики» ежегодно будет направляться порядка 20 млрд руб. Реализация нацпроектов подтолкнет внутреннее потребление услуг центров обработки и хранения данных, облачных сервисов, обеспечит рост объема данных и спрос на вычислительные мощности.

Важно, чтобы бизнес не пошел по пути создания/расширения собственной вычислительной инфраструктуры, но начал приобретать инфраструктурные сервисы на рынке. Для этого необходимо стимулировать более широкое распространение сервисной модели потребления инфраструктуры ЦОДов (вместо использования собственной инфраструктуры) организациями государственного и коммерческого секторов.

Если потенциал российского рынка дата-центров не будет реализован, он так и останется незаметным в глобальном масштабе. Международные гиперЦОДы уже сейчас агрессивно делят между собой мировой рынок, в том числе обслуживая потребности российских клиентов. Сегодня условия благоприятствуют тому, чтобы изменить сложившуюся ситуацию.

КОЛОНКА ЭКСПЕРТА

Фото: facebook.com/IXcellerate

Edge: близко, ближе, совсем рядом

Тема edge computing обещает стать главной в ИТ на ближайшие годы. Ограниченность ширины каналов связи и скорости передачи сигнала при стремительном росте объемов данных настоятельно требует приближения ЦОДов к местам, где данные генерируются и потребляются.

Как любая новая и перспективная технология, edge computing окружена огромным числом мифов, домыслов и, так скажем, элементов технологического гламура. Таблоиды полны громких заголовков типа «Edge – убийца облака», а аналитики соревнуются в придумывании все новых и новых архитектур, чтобы изящно вписать туда edge. Например, The Cerebrus Group предлагает архитектуру Edge–Edgier–Edgiest, а IDC выделяет уровни Light Edge, Heavy Edge и Packaged Endpoint. Я использую английские термины, потому как перевод на русский не устоялся и может еще больше запутать ситуацию. Пограничные, периферийные, распределенные вычисления – вот только некоторые из возможных переводов.

Выработке единого понимания, столь важного для конечных заказчиков, всегда помогает общение профессионалов на конференциях и форумах. Почти сразу после московского форума «ЦОД-2019», на котором технология edge computing стала главной темой, я посетил конференцию Life at the Edge, организованную Schneider Electric в Сингапуре. Место проведения – культовое для ИТ. Самый «умный» город планеты (по данным Juniper Research за 2015 г.), Сингапур занимает первое место в мире по развитию ИТ. Все, что можно автоматизировать, там уже автоматизировано или будет автоматизировано в ближайшее время. Электронной визой, беспилотными поездами метро или отсутствием персонала на стойках регистрации и приема багажа в аэропорту, возможно, удивить уже нельзя. Но вот прохождение пограничного контроля без пограничника меня действительно поразило...



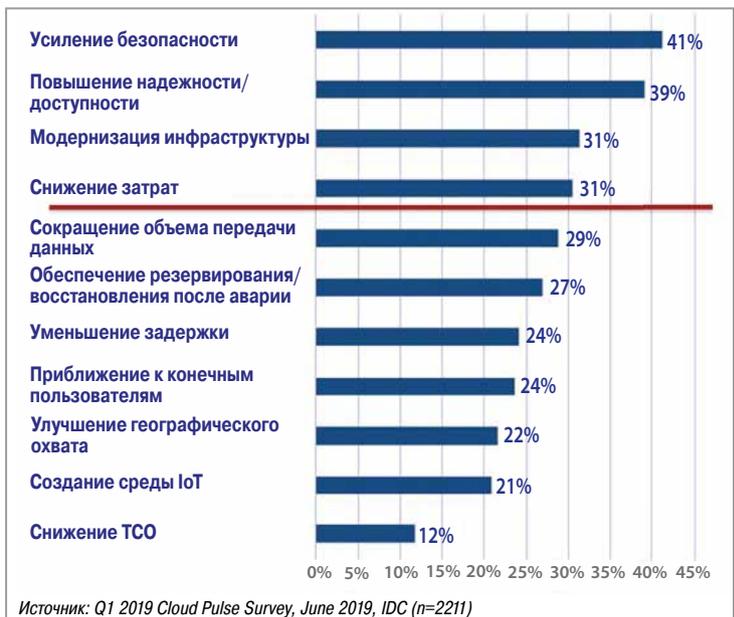
▲ Рис. 1. Где сегодня компании обрабатывают IoT-данные

Заказчики (не)готовы

По прогнозу Gartner, к 2025 г. 75% данных будут генерироваться и обрабатываться предприятиями на границе ИТ-инфраструктуры, на edge-уровне. Сегодня, по данным IDC, только 26% организаций в мире анализируют IoT-данные на уровне edge, еще 35% используют edge-узлы для первичной обработки, результаты которой направляются в корпоративные ЦОДы. Большинство – 37% – пересылают такие данные сразу в классические ЦОДы (рис. 1).

Хотя производители и аналитики вовсю пропагандируют edge computing как будущее ИТ, заказчики пока не слишком готовы к новой архитектуре. 60% опрошенных IDC не имеют стратегии для реализации этой концепции. У тех же, кто такую стратегию разработал, основные затруднения вызывает обеспечение безопасности. Помимо безопасности сомнения относительно внедрения IoT-решений связаны со стабильностью имеющихся платформ, достижением приемлемой стоимости владения, а также с квалификацией собственных сотрудников.

Каким бы противоречивым это не выглядело, но среди основных причин, по которым компании перемещают приложения на уровень edge, – надежды на улучшение безопасности и снижение стоимости инфраструктуры. Также они рассчитывают на повышение надежности и доступности своих ИТ-систем (рис. 2).



▲ Рис. 2. Основные драйверы Edge Computing



Архитектурные вопросы

Эксперты Schneider Electric предлагают относительно простую иерархию ЦОДов: крупные (мега- или гипер-) дата-центры, региональные и локальные edge-ЦОДы (рис. 3). Предполагается, что крупные ЦОДы размещаются вне больших городов, по возможности в местах, приближенных к источникам электроэнергии. Место для региональных edge-ЦОДов – как раз крупные города. Наконец, локальные «эджи» размещаются там, где данные генерируются и потребляются.

В качестве сред развертывания локальных edge-ЦОДов выделяют три основных варианта: промышленные (жесткие) условия; коммерческие и офисные здания; специализированные ИТ-помещения. Технические решения подбирают с учетом условий эксплуатации. Так, для установки в жестких условиях, например в производственном цеху, рекомендуется использовать микро- или модульные ЦОДы, выполненные в хорошо защищенных корпусах. В специализированных ИТ-помещениях, где уже созданы условия для эксплуатации ИТ-оборудования, могут устанавливаться как те же микроЦОДы, но уже в корпусах с меньшим уровнем защиты, так и традиционные рядные решения, которые обычно размещаются в крупных ЦОДах. Под микроЦОДом обычно понимают решение, реализованное в формфакторе одной стойки или ее части (например, в корпусе, рассчитанном на 6U). Наиболее известный пример модульного ЦОДа – это ЦОД-контейнер.

Маленький не значит ненадежный

Традиционно определение надежности дата-центров основывается на оценке доступности отдельных площадок. Такой подход абсолютно оправдан, если используется один ЦОД. Но когда на смену централизованной модели приходит распределенная, надо говорить о надежности всей сети ЦОДов. А надежность системы, как известно, определяется характеристиками самого ненадежного узла. Кевин Браун, старший вице-президент по инновациям подразделения Secure Power компании Schneider Electric, призвал рассматривать edge-узлы как критически важные дата-центры. В качестве примера он привел сеть ЦОДов, в которой основной дата-центр соответствует требованиям Tier 3, а периферийные – Tier 1. ЦОДы Tier 3 характеризуются временем простоя не более 1,6 ч в год. Однако соответствующий показатель всей системы будет определяться объектами Tier 1 и составит 30,7 ч в год.

Низкий уровень надежности большинства периферийных комплексов – наследие прошлого. Незащищенные стойки, отсутствие резервирования и выделенной системы охлаждения – вот традиционные проблемы таких площадок. Ситуацию усугубляет отсутствие современной системы мониторинга и управления, что при дефиците квалифицированного персонала на удаленных объектах и определяло удручающие эксплуатационные показатели. Судите сами, если до объекта инженеру



◀ **Рис. 3.**
Архитектура
распределенной
сети ЦОДов,
предлагаемая
Schneider Electric

Источник: Schneider Electric



▲ Рис. 4. В демоцентре Schneider Electric в Сингапуре

нужно добираться несколько часов или даже дней, а средства дистанционного мониторинга/управления отсутствуют, то о доступности уровня Tier 3, да и Tier 2, говорить не приходится.

Как же изменить ситуацию?

Интеграция и управление

Эксперты Schneider предлагают три основных направления работы на рынке edge-решений. Первое – предоставление заказчикам интегрированного, максимально готового к развертыванию решения. Сама компания, производя все основные компоненты инженерной инфраструктуры для ИТ, уже давно поставляет комплексные решения. Для edge computing это могут быть уже упомянутые микро- или модульные ЦОДы со всем необходимым оборудованием, представленные, в частности, в демоцентре в Сингапуре (рис. 4).

Следующий шаг – плотное сотрудничество с ключевыми поставщиками ИТ-оборудования, что выводит интеграцию на новый уровень: заказчик получает не только решение с установленной «инженеркой», но и серверы, СХД и другие необходимые ИТ-компоненты.

«Ни один вендор в одиночку не способен обеспечить полное решение. Нужна экосистема», – убеждена Наталия Макарошкина, старший вице-президент подразделения Secure Power компании Schneider Electric в регионе International. Альянсы с другими производителями, среди которых – VMware, Cisco, HPE, Dell, Lenovo, NetApp и т.д., позволяют Schneider Electric поставлять готовые решения, включая серверы. При таком подходе все участники проекта получают выгоду. Интеграторы проекта могут значительно снизить инженерные затраты на раз-

вертывание и поддержку edge-ЦОДов, а заказчик существенно сократит время на реализацию проекта без риска потерять гарантию со стороны производителей ИТ-оборудования. При этом, по словам Н. Макарошкиной, экосистема важна на всех этапах, не только при реализации проекта, но и при дальнейшем обслуживании объекта.

Третье направление связано с развитием систем управления. Ахиллесовой пятой современных ИТ-комплексов на удаленных площадках является недостаток средств дистанционного мониторинга/управления при нехватке квалифицированного персонала на местах. Как считает Кевин Браун, традиционные средства управления не позволяют эффективно решать задачи на edge-уровне. Он уверен в том, что современные инструменты управления должны базироваться на облачной модели, а для помощи персоналу на удаленных площадках нужно активно использовать аналитику и искусственный интеллект. Именно над внедрением соответствующих компонентов активно работают специалисты Schneider Electric, развивая свою систему управления EcoStruxure IT, которую они позиционируют как решение DCIM нового поколения.

...Пора прощаться с цифровым Сингапуром. Аэропорт Чанги, пограничный контроль без пограничников: прикладываешь большой палец к сканеру, система все проверяет и пожалуйста – вы в зоне дьюти-фри. Впереди 10-часовой перелет в Москву, но благодаря современным технологиям и он проходит быстро – мультимедиа-комплекс в спинке стоящего впереди кресла в авиалайнере Singapore Airlines впечатляет своим функционалом, за которым – серьезная ИТ-начинка. Современный авиалайнер – это тоже edge-объект.

**Александр Барсков,
Сингапур – Москва**

Ноябрь

пн	вт	ср	чт	пт	сб	вс
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

Декабрь

пн	вт	ср	чт	пт	сб	вс
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

2020

Январь

пн	вт	ср	чт	пт	сб	вс
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

Февраль

пн	вт	ср	чт	пт	сб	вс
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	

Март

пн	вт	ср	чт	пт	сб	вс
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

27–28 ноября. Ашхабад, Туркменистан

TurkmenTEL. Turkmenistan Telecommunications & IT Conference 2019

Министерство промышленности и связи Туркменистана
www.turkmenistantelecoms.com

28 ноября. Екатеринбург

2-я международная конференция и выставка «ЦОД: модели, сервисы, инфраструктура»

ИКС-МЕДИА
ekb.dcforum.ru



29 ноября. Москва

Телеком Форум РБК 2019

РБК
bc.rbc.ru/event/5d08f1b39a7947cd38e08edd

29 ноября. Москва

Международное соревнование и акселератор для создания новых цифровых сервисов и продуктов Urban Tech Moscow

Правительство Москвы, Департамент предпринимательства и инновационного развития г. Москвы, Агентство инноваций г. Москвы
innoagency.ru/utm

29 ноября. Москва

Международный форум по цифровизации промышленности Digital Industry Forum

Фонд развития цифровой экономики
forum.digital/industry

29–30 ноября. Москва

5-я международная конференция по информационной безопасности Skolkovo Cyberday 2019

Фонд «Сколково», АРСИБ
cyberday.sk.ru

5 декабря. Москва

Пиринговый форум MSK-IX 2019

MSK-IX
www.msk-ix.ru

6 декабря. Санкт-Петербург

Internet of Things Forum

Garant Group
iot-forum.ru

9–10 декабря. Москва

3-й международный научный форум «Шаг в будущее: искусственный интеллект и цифровая экономика»

Государственный университет управления
aiforum.guu.ru

12–13 декабря. Москва

Russian Internet Week

РАЭК, РОЦИТ, Институт развития интернета, Министерство цифрового развития, связи и массовых коммуникаций РФ
riw.moscow

28–30 января 2020 г. Москва

22-я международная выставка и форум телевидения и телекоммуникаций CSTB Telecom & Media

«Мидэкспо»
www.cstb.ru

30–31 января. Москва

22-й большой национальный форум информационной безопасности «Инфофорум-2020»

«Инфофорум»
infoforum.ru/conference/2020

11–13 февраля. Москва

Международный форум «Технологии безопасности» ТБ ФОРУМ 2020

«Гротек»
www.tbforum.ru

12–14 февраля. Сочи

Российский инвестиционный форум

Росконгресс
rusinvestforum.org

27 февраля. Москва

Российский цифровой форум

Фонд развития цифровой экономики
forum.digital

26 марта. Москва

9-я международная конференция и выставка Cloud & Digital Transformation

ИКС-МЕДИА
cloud-digital.ru

CLOUD & DIGITAL
TRANSFORMATION

ВЭФ-2019 как зеркало контрастов Дальнего Востока



Татьяна Толмачева, партнер, iKS-Consulting

Уникальные природные богатства – и громадные территории, не охваченные сотовой связью. Трллионы рублей инвестиций в нефтегазопереработку, энергетику и транспорт – и миллиарды в формирование цифровой инфраструктуры. Как будет развиваться цифровизация региона?

Особенный Дальний Восток

Дальний Восток – регион в силу многих факторов не обычный и не простой. Его формируют 11 субъектов Российской Федерации, охватывающие в сумме более 40% территории нашей страны, но проживает там менее 6% ее населения (данные 2018 г.). Википедия называет регион «самым депопулирующим»: в течение последних 15 лет отток молодежи стабильно растет, несмотря на то что на всем протяжении освоения Дальнего Востока для удержания населения и привлечения рабочей силы предлагались специальные льготы и преференции.

На сегодня все входящие в состав Дальнего Востока субъекты РФ являются дотационными. Вклад региона в российскую экономику достаточно скромный, хотя на его территории находятся крупнейшие запасы сырья.

Ключевые проблемы Дальнего Востока – его транспортная изоляция от остальной части страны, низкий уровень инновационности региональных экономик, низкое качество социальной инфраструктуры и низкий уровень жизни населения.

На изменение текущей ситуации направлена Стратегия социально-экономического развития Дальнего Востока и Байкальского региона на период до 2025 г., утвержденная Правительством РФ в конце 2009 г. А в феврале 2019 г. была принята Стратегия пространственного развития до 2025 г., цель которой – повысить геополитическое значение Дальнего Востока, его роль и место в политическом, экономическом и социальном развитии России, изменить структуру экономики, усилить интеграцию в АТР. Предполагается сформировать центры экономического роста таким образом, чтобы каждый регион имел свою экономическую специализацию. Осо-

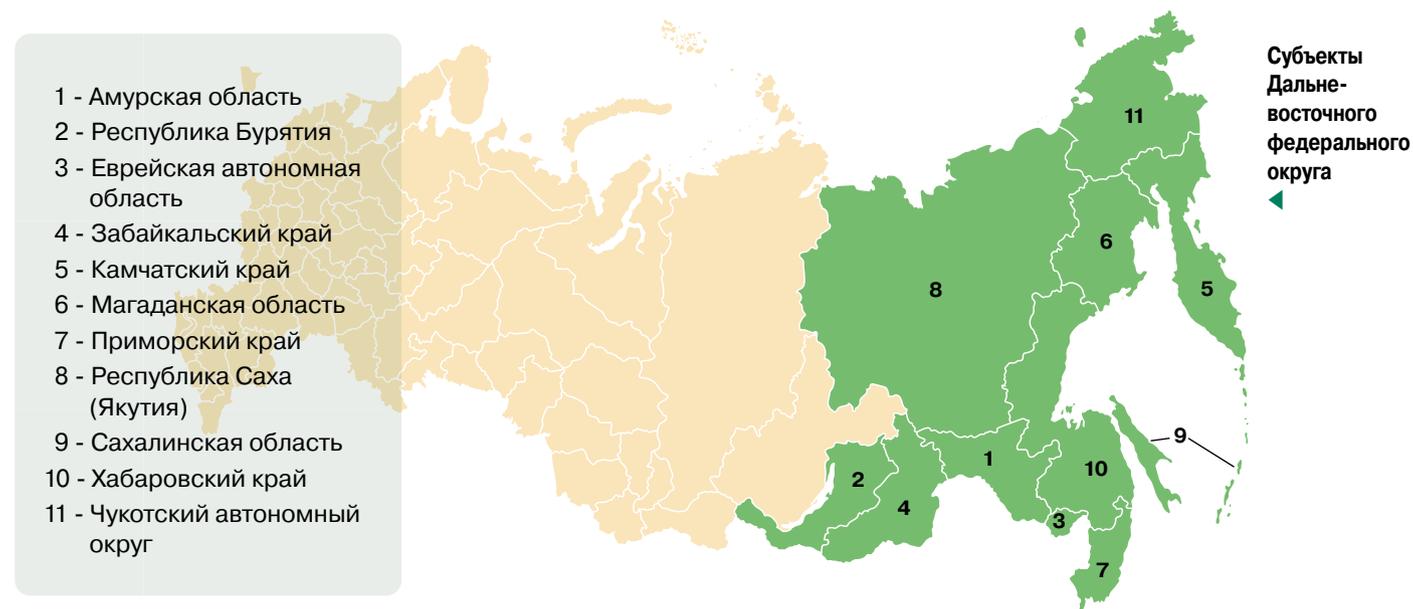
бое внимание уделяется развитию транспортной и энергетической инфраструктуры, освоению ресурсного потенциала.

В настоящее время на Дальнем Востоке реализуются масштабные инвестиционные проекты на основе государственно-частного партнерства, нацеленные на решение стратегических задач. В качестве примера можно привести Восточную газовую программу – государственную «Программу создания в Восточной Сибири и на Дальнем Востоке единой системы добычи, транспортировки газа и газоснабжения с учетом возможного экспорта газа на рынки Китая и других стран АТР» (принята в 2007 г.). Цель программы – формирование новых центров газодобычи и системы транспортировки газа, нового канала экспорта российского газа в страны АТР.

Развитие информационно-телекоммуникационной инфраструктуры и информационно-телекоммуникационная безопасность выделены в отдельные направления стратегического развития дальневосточных регионов.

Инвестиционные проекты на Дальнем Востоке

- Р** Амурский газоперерабатывающий завод («Газпром», 950 млрд руб.)
- Р** Восточный нефтехимический комплекс («Роснефть», 700 млрд руб.)
- Р** Амурский газохимический комплекс (СИБУР, 600 млрд руб.)
- Р** Находкинский завод минеральных удобрений («Национальная химическая группа», 390 млрд руб.)
- Р** Судостроительный комплекс «Звезда» (консорциум инвесторов, 200 млрд руб.)
- Р** Наталкинский ГОК («Полус», 82 млрд руб.)



ИКТ-инфраструктура для цифрового Дальнего Востока

ИКТ-отрасль на Дальнем Востоке представлена как небольшими локальными операторами связи, так и всеми крупнейшими федеральными компаниями («Ростелеком», МТС, «Вымпелком», Orange Business Services, «ТрансТелеКом» и др.). Связь в регионе, как и по стране в целом, развивалась по принципу экономической целесообразности – капиталовложения в создание инфраструктуры делались только с условием достижения целевых показателей окупаемости, возврата инвестиций и прибыльности.

Поэтому информационно-телекоммуникационная инфраструктура, которая должна обеспечивать цифровую трансформацию экономики региона, развита очень неравномерно: она хорошо сформирована вдоль транспортных магистра-

ЦОДов в регионе можно пересчитать по пальцам одной руки: «Ростелеком», «Рэдком» (Хабаровск), «Порттелеком» (Владивосток), «Иркутскэнерго-связь» (Иркутск). Операторы связи имеют небольшие дата-центры типа серверных комнат. При этом серверные мощности операторов в основном обслуживают их внутренние потребности. Например, мощности «Ростелекома» на 90% используются компанией для собственных нужд.

Потребности в инфраструктуре ЦОДов обеспечивают также дата-центры региональных администраций и корпоративные дата-центры крупных компаний. Все федеральные компании, реализующие масштабные инвестиционные проекты на Дальнем Востоке («Газпром», «Роснефть», СИБУР и др.), имеют собственные корпоративные центры обработки и хранения данных (как правило, расположенные поближе к штаб-квартирам), которые удовлетворяют текущие потребности региона.

Коммерческих ЦОДов с высокой степенью отказоустойчивости на Дальнем Востоке нет.

Очевидно, что реализация крупных инвестиционных проектов, способствуя развитию региона в целом, будет стимулировать рост спроса на инфраструктуру ЦОДов. Тот же эффект должна дать и государственная политика в области ЦОДостроительства. Не случайно ряд компаний и регионов планируют инвестировать в строительство и дальнейшее развитие цифровой инфраструктуры, в том числе инфраструктуры центров обработки и хранения данных. Например, о своих планах строительства к 2020 г. в Хабаровске регионального дата-центра объявил «Ростелеком». Якутия намерена построить для электронного правительства республики новый ЦОД, который, по мнению местных властей, может стать одним из самых крупных на Дальнем Востоке.

Взгляд ИКТ-аналитика на ВЭФ-2019

В начале сентября во Владивостоке состоялся пятый Восточный экономический форум. ВЭФ учрежден в 2015 г. как один из инструментов решения задач пространственного развития Дальнего Востока и его интеграции в Азиатско-Тихоокеанский регион.

Форум уже стал важным событием в жизни Дальнего Востока. Это площадка, где сообщают об успехах в выполнении обнародованных ранее планов, делают программные заявления, проводят встречи на высоком уровне, достигают важных договоренностей относительно дальнейшего сотрудничества. ВЭФ является площадкой для встреч государства с международным и российским частным бизнесом.

В этом году на выставке в рамках форума в качестве экспонентов были представлены все регионы Дальнего Востока, отдельные федераль-

Президент, председатель правления ПАО «Ростелеком» Михаил Осеевский во время сессии «Цифровое государство: новые бизнес-модели на волне тотальной цифровизации»



Источник: Фотохост-агентство ТАСС/Красильников Станислав

Соглашения, подписанные «Ростелекомом» на ВЭФ 2019:

- о сотрудничестве с правительством Камчатского края
- сотрудничестве с Дальневосточным фондом высоких технологий
- сотрудничестве с правительством Кузбасса
- сотрудничестве с правительством Республики Саха
- сотрудничестве с «Золоторудной компанией Павлик»
- сотрудничестве с ООО «Газпром газэнергосеть гелий»
- создании Дальневосточного центра Киберполигона «Ростелекома»

лей федерального уровня, а также в крупных административных центрах, где есть платежеспособный спрос. При этом часть автомобильных дорог регионального значения, проходящих по удаленным местностям, находится вне зоны покрытия сотовой связи. А значит – для отдельных территорий Дальнего Востока все еще актуально создание даже базовой телеком-инфраструктуры. На решение этой задачи ориентирована государственная политика (федеральный проект «Информационная инфраструктура», механизм системы универсального обслуживания).

Текущие потребности в инфраструктуре центров обработки данных на Дальнем Востоке закрывают операторы связи. Это одна из услуг в их продуктовом портфеле. Но поставщиков услуг



Подготовка к открытию V Восточного экономического форума

ные ведомства, большинство корпораций с государственным участием и российские институты развития.

Для участия в форуме необходимо сделать достаточно крупный регистрационный взнос, что вкупе с расходами на проезд и проживание складывается в немалую сумму, которую могут себе позволить только те частные компании, для которых Дальний Восток является стратегическим регионом, а государство – важным партнером для ведения бизнеса.

Ключевые темы форума – международное сотрудничество, развитие транспортной и энергетической инфраструктуры, различные аспекты реализации инвестиционного потенциала региона. В нынешнем году темы развития цифровой инфраструктуры и цифровизации экономики хотя и не были «якорными», присутствовали во всех треках деловой программы форума.

Показателем эффективности проведенного мероприятия можно считать количество подписанных соглашений. Организаторы форума отчитались о заключении 270 соглашений на сумму 3,4 трлн руб.

В рамках форума был подписан ряд соглашений, которые должны стать драйвером развития цифровой инфраструктуры на Дальнем Востоке. Среди прочих хочется отметить соглашение о создании на базе Дальневосточного федерального университета инновационного научно-технологического центра «Русский» (ИНТЦ «Русский»), включающего центр цифрового разви-

Первые проекты Центра цифрового развития:

- ✓ Создание Киберполигона и центра тестирования программного обеспечения («Ростелеком»)
- ✓ Цифровое моделирование процессов сжижения газа, его подводной добычи и развитие робототехники («Газпром»)
- ✓ Развитие промышленных и цифровых технологий в вертолетостроении («Вертолеты России»)
- ✓ Создание цифровых двойников исследовательских установок («Росатом»)
- ✓ Разработка облака больших геологических данных, алгоритмов и программных решений для анализа больших данных в области геологии («Росгеология»)
- ✓ Создание цифровых двойников железнодорожной инфраструктуры и обработка больших данных в интересах кадровых подразделений компании (РЖД)
- ✓ Создание Центра коллективного проектирования электронной компонентной базы («Элемент»)
- ✓ Создание цифрового двойника Владивостока (МТС)

тия, центр коллективного проектирования электроники «Восток», инжиниринговые центры, центры исследований и разработок с участием российских госкорпораций и ведущих ИТ-компаний. ИНТЦ «Русский» станет дальневосточным ИТ-кластером, который объединит компетенции в области «сквозных» цифровых технологий.

ДВФУ будет формировать на о. Русском экосистему технологического предпринимательства для инновационного развития региона, которая обеспечит научно-технологический прорыв не только для Дальнего Востока, но и для России в целом.

Темы выступлений на ВЭФ-2019, посвященных цифровой инфраструктуре и цифровой экономике:

- Инфраструктура для экономики данных
- Цифровая инфраструктура для создания комфортной среды проживания населения
- Цифровые транспортные коридоры
- Цифровая медицинская помощь для повышения качества жизни
- Цифровая трансформация строительной отрасли
- Цифровая трансформация международной торговли
- Новые бизнес-модели в цифровом государстве
- Цифровые технологии в образовании



▲ Министр цифрового развития, связи и массовых коммуникаций РФ Константин Носков и президент ПАО «МТС» Алексей Корня (слева направо) во время церемонии подписания соглашения

Предполагается, что финансировать проекты будут сами компании за счет собственных средств с возможностью получения на конкурсной основе мер господдержки в рамках нацпрограммы «Цифровая экономика Российской Федерации».

МТС подписала целый ряд соглашений с региональными правительствами (с администрациями Бурятии, Якутии, Камчатки, Сахалинской, Амурской областей и Хабаровского края) о развитии цифровой инфраструктуры регионов. Общий объем инвестиций МТС в развитие этих регионов до 2021 г. должен превысить 3 млрд руб. В число инвестиционных проектов войдут: создание сетей NB-IoT, пилотных зон для тестирования цифровых продуктов и вертикальных решений в области цифровизации городского хозяйства («умный город»), анализ данных с целью развития социальной и туристической инфраструктуры и т.д. Одно из крупнейших подписанных на форуме инвестиционных соглашений в сфере цифровизации – это соглашение МТС с администрацией Хабаровского края о капиталовложениях в цифровизацию региона в объеме 1,4 млрд руб. до конца 2021 г.

Однако в ходе форума было подписано и много протокольных соглашений о сотрудничестве, без конкретики и деталей.

Нельзя не отметить, что размеры инвестиций в развитие цифровой инфраструктуры не сравнимы с инвестициями в проекты обрабатывающей промышленности, транспортной или энергетической инфраструктуры. На фоне мегапроектов «Газпрома», «Роснефти», СИБУРа и других сырьевых компаний инвестиции в цифровизацию практически незаметны. А значит, тема цифровизации и цифровой инфраструктуры никогда не будет в программе ВЭФ ключевой.

Тем не менее интерес к созданию цифровой инфраструктуры и цифровой экономики, сти-

мулированию технологического развития Дальнего Востока был высок. Степень интереса можно оценить по количеству участников Форума, которые имеют отношение к инфотелекоммуникационной отрасли, количеству тематических выступлений, наличию в деловой программе отдельных сессий, посвященных цифровизации и цифровой инфраструктуре, по активному участию Министерства цифрового развития, связи и массовых коммуникаций в мероприятиях Форума. Под эгидой Минкомсвязи России была подготовлена и проведена панельная дискуссия «Инфраструктура для экономики данных».

Говоря об инвестициях в развитие Дальнего Востока, называют огромные суммы – триллионы рублей. Источники финансирования большинства проектов – корпорации с государственным участием и бюджеты развития. Важно, чтобы совершенствование транспортной и энергетической инфраструктуры, ресурсные и производственные проекты были взаимосвязаны с задачами формирования инфокоммуникационной инфраструктуры как неотъемлемой их части.

Координирует деятельность по реализации государственных и федеральных целевых программ развития Дальнего Востока специально созданная мощная административная структура – «Большое министерство» – Министерство Российской Федерации по развитию Дальнего Востока и Арктики и подведомственные ему организации, в числе которых Агентство Дальнего Востока по привлечению инвестиций и поддержке экспорта, Корпорация развития Дальнего Востока, Агентство по развитию человеческого капитала на Дальнем Востоке, Восточный центр государственного планирования.

Все увиденное и услышанное на Восточном экономическом форуме-2019 вызывает двойственные чувства. С одной стороны, гуляя по просторному и ультрасовременному кампусу ДВФУ, осматривая экспозиции «Улицы Дальнего Востока», проезжая по мосту на о. Русский, испытываешь чувство восхищения и гордости.

С другой стороны, вспоминаешь, что с 2005 г., когда был разработан инвестиционный проект «Развитие о. Русский», прошло уже почти 15 лет. Практически все построенные на острове в последние годы объекты так или иначе связаны с саммитом АТЭС, который проходил во Владивостоке семь лет назад. Остров Русский уже прозвали «территорией бесконечного развития».

Хочется надеяться, что всем заявленным планам суждено сбыться и в результате их реализации удастся переломить тренд депопуляции и Дальний Восток станет не только цифровым, но и привлекательным для проживания регионом. ИКС

Может ли Россия стать крупным поставщиком ПО для целых регионов мира?



Ответ на этот вопрос будет зависеть от того, сможет ли наша страна эффективно поддерживать создание множества новых программных продуктов, ориентированных на экспорт.

Светлана Гацакова,
директор
департамента
корпоратив-
ных инфор-
мационных
систем,
ALP Group

Отношение к экспорту российского ПО постепенно меняется – от недоверия и изначального пессимизма к удивлению по поводу неожиданно большого числа существующих отечественных программных технологий и продуктов (спасибо реестру российского ПО!), а потом и к появлению уверенности в своих силах, основанной на разработке импортнезависимых технологических платформ и на успешном выполнении ряда крупных проектов информатизации в коммерческом секторе, госсекторе и силовых структурах.

Однако здесь надо четко разделять две точки приложения сил государства. Первая – это поддержка продвижения на зарубежные рынки уже созданных российских программных продуктов и технологий (например, антивирусного ПО, платформ для разработки систем ERP и i-ERP и др.). Вторая – обеспечение условий для создания новых программных продуктов и технологий с большим экспортным потенциалом, включая разработки для цифровизации всего. Это совершенно разные проблемы, и инструменты их решения тоже совершенно разные.

Поддержка экспорта готового ПО

Думаю, в 2019 г. не нужно много говорить о необходимости такой поддержки. Достаточно вспомнить ожесточенную кампанию по дискредитации российских разработчиков, созданию образа врага, накрепко связанного с криминалом, шпионажем, манипулированием выборами

и различными общественными процессами... Но медийным пространством противостояние уже не ограничивается. Вспомним, как США поступили с продукцией «Лаборатории Касперского». Их просто выгнали, используя методы, весьма далекие от честной конкуренции. Еще круче обошлись с высокотехнологичными китайскими гигантами. Как только Huawei стала претендовать на лидерство в целом ряде сегментов, включая смартфоны, начались санкции, запреты, последовал арест одного из высших должностных лиц и появились удивительное предложение «договориться» и решительное карающее воздействие через «корпорацию добра».

Это вовсе не отдельные случаи, а набирающая обороты практика устранения сильных конкурентов политическими методами. Очевидно, что США и зависимые от них западные страны не ограничатся защитой собственных рынков, а будут тайно и явно использовать весь арсенал имеющихся у них средств, чтобы затруднить работу российских компаний на перспективных рынках в других регионах мира: на Ближнем Востоке, в Южной Америке и Юго-Восточной Азии. Это уже не просто высокая цена вхождения на рынок, это обстоятельства, с которыми коммерческое предприятие, даже самое крупное, не может справиться в принципе. Здесь необходимо серьезное участие государства, выходящее далеко за границы компенсации затрат на продвижение продукции.

Однако при всей важности поддержки экспорта готовых российских программных продуктов для имиджа страны их количество невелико и само по себе существенно увеличиться не может. Поэтому решающее значение для того, станет ли Россия первоклассным экспортером ПО, будет иметь именно поддержка создания множества новых программных продуктов, ориентированных на экспорт.

Главное – о чем мечтает молодежь

Для того чтобы Россия стала центром экспорта мирной продукции в сфере высоких технологий, государство должно энергично, масштабно и системно поддерживать сам процесс разработки конкурентной высокотехнологичной продукции, уделяя внимание не какой-то одной, а всем его стадиям.

Как этого добиться? Первый шаг более или менее очевиден. Как, например, китайцы поднимают свой автопром, да и телеком тоже? Начали с копирования машин, разработанных ведущими автопроизводителями. Не можешь придумать сам – подсмотри у соседа. Я не призываю к пиратству! Есть вполне легальные формы заимствования. Google сделала голосового помощника, и у «Яндекса» тут же появилась «Алиса». Алгоритмы другие, но идея та же. Можно вспомнить опыт индустриализации СССР, когда концессии, выдаваемые иностранным компаниям, использовались не только для создания промышленных объектов, но и для обучения кадров, что позволяло в масштабах целой страны перенять практики, ускоренно вовлечь в новые отрасли большие массы людей и приучить их к технологической дисциплине. Сегодня есть и другой, вполне легальный путь – open source. Это великое разнообразие технологий и продуктов, среди которых немало первоклассных. Open source дает возможность изучать информационную архитектуру и программный код, участвовать в работе международных сообществ, которые эти продукты развивают, пользоваться теми же инструментами и методиками. Участие в таких сообществах – не только отличная школа, но и возможность создать себе имя, ведь все сделанное человеком становится известно, формирует его репутацию.

Не обидно ли нам, запустившим в космос первого космонавта, идти по этому пути? По-моему, нет. В области мирной высокотехнологичной продукции (включая программные продукты) и ведения основанного на ней крупного международного бизнеса мы сильно отстали от США, Западной Европы, Японии, современного Китая. Образовавшийся разрыв трудно преодолеть. Переложить эту задачу на ИТ-компании или на госкорпорации нельзя. Нужны супермеры, главная цель которых лежит в области общественно-

го сознания. Нужно избавиться от пессимизма, сформировать в обществе веру в возможность превратить Россию в экспортера ПО и воспитать поколения, которые хотели бы стать инженерами и участвовать в достижении этой цели.

Начинать надо издали: создавать и поддерживать инженерные классы в школах и школы инженерного профиля, вести в школах, вузах, коворкингах проекты, связанные с ИТ, чтобы каждый желающий мог в них участвовать. И главное – необходимо направлять мышление молодого поколения в сторону инженерии, выявлять, развивать и воспитывать людей, которые вообще способны придумать что-либо. Это большая задача, которую государство уже начало выполнять и которой планирует заниматься во все больших масштабах. Но, на мой взгляд, самое главное – увеличить размах популяризации, которая должна дотягиваться до каждой семьи.

Популяризация работает

У всех нас перед глазами есть пример того, что целенаправленная популяризация (в сочетании с созданием инфраструктуры) действительно работает. Так, была задача по спорту – чтобы наши спортсмены победили в Олимпийских играх. Были приняты масштабные меры, давшие необходимый результат:

- крупные спортивные объекты, ранее отданные под рынки, вернули обратно в спорт, реконструировали и подняли до высокого уровня (во многих случаях – до мирового);
- разработали план строительства новых спортивных объектов и выполнили его;
- развернули поддержку детского спорта, в рамках которой открыли клубы и секции, в каждом дворе отремонтировали спортивные площадки и почти в каждом дворе – «коробки» для игровых видов спорта: футбола, хоккея и др.;
- придумали и раскрутили программы на телевидении, например разные ледовые шоу, чтобы дети захотели стать фигуристами, гимнастами и т.п.

В частности, нашли способ вернуть популярность фигурному катанию. В одном из ледовых шоу новичок, ни разу не стоявший на коньках, за три месяца под присмотром опытного фигуриста добивался отличных результатов – мог не просто кататься, но и выполнять достаточно сложные фигуры. Все увидели, и дети тоже, что этих результатов, которые они считали совершенно невозможными, можно, оказывается, добиться за совсем короткий срок. Все поняли: да, это возможно. И многие дети пошли в фигурное катание, нацелились на серьезные результаты.

То же самое (конечно, по сути, а не по форме) нужно делать и в области информационных технологий: придумывать и проводить мероприятия, затевать зрелищные проекты, затрагивающие

разработку высокотехнологичных продуктов, связать их с картиной будущего нашей страны и других регионов, провести параллели с достижениями прошлого, которыми все мы продолжаем гордиться. Молодежь устала от дефицита настоящих смыслов, примитивный культ потребления не может их заменить. Этот дефицит смыслов надо правильно заполнить.

В то же время современные молодые люди смотрят на жизнь прагматично. И если мы не хотим экспортировать само это поколение (и их потомков), надо подумать и о престиже профессии инженера, и о действительно высоком уровне жизни для тех, кто выбрал этот нелегкий путь и шаг за шагом идет по нему.

Человек должен поверить (и не разочароваться в этом в дальнейшем), что если он придумал что-либо действительно ценное, что привлечет инвесторов и станет основой успешного экспортного проекта, то коммерческие компании не заберут себе всё. Что изобретатель, автор идеи, технологии или продукта может получать за них деньги и стать уважаемым членом общества. Было бы отлично, если бы всё это было убедительно показано, как в случае фигурного катания: вот ты ничего не умел, вот ты катаешься на коньках, а вот ты фигурист. И на всё это потребовалось три месяца плюс упорство и сотрудничество с наставником.

Какие продукты имеют экспортный потенциал

Отмечу еще одну проблему, связанную с трудностью создания продуктов с высоким экспортным потенциалом. Нет такого человека, который сел бы и написал: вот такие высокотехнологичные продукты будут хорошо экспортироваться туда-то, а такие – туда-то. И процедуры, выявляющей эти продукты, тоже нет. А значит, нельзя запустить и госпрограмму поддержки создания конкретных продуктов.

Лучше направить усилия (и ресурсы) на улучшение информирования разработчиков о социальных и экономических процессах на целевых рынках (так как именно такие процессы и изменения время от времени формируют «окна возможностей»). А в долгосрочной перспективе – на подготовку хороших специалистов, верящих в свои силы, а также на создание условий, когда они «варятся в одном котле», постоянно генерируют перспективные идеи и пробуют претворить их в жизнь, иногда добиваясь успеха, а иногда обжигаясь.

У нас есть «Сколково», созданное именно для того, чтобы помогать компаниям разрабатывать высокотехнологичные инновационные продукты. Но пока этот проект, несмотря на огромные ресурсы, не дает сверхуспешных результатов, когда российское ПО успешно продавалось бы за рубежом. Видимо, надо плотно заняться начальными звеньями процесса разработки высокотехнологичной продукции – воспитанием специалистов в том ключе, о котором я говорила выше. **ИКС**



Энергия интеллекта

Ведущее аналитическое агентство России и СНГ в сфере телекоммуникаций, ИТ и медиа

- Аналитика
- Стратегии
- Бизнес-планирование
- Информационно-аналитическая поддержка
- Потребительские опросы в B2C и B2B сегментах



Лондон



Киев



Москва



Алматы

ИТ

Телеком

Медиа

Контент и сервисы

Системная интеграция

Голосовые услуги

Платное ТВ

Навигация и LBS

Дата-центры

ШПД

Мобильное видео

M2M

Облачные сервисы

Мобильный интернет

Игры

NFC

ИТ инфраструктура

VAS

Интернет-порталы

E-commerce

Офисная техника

Межоператорские услуги

Видео-контент

Теле-медицина

Оцифровать урожайность



Денис Васюков, специалист по системам точного земледелия и защите растений, John Deere

В 2018 г. аграрный сектор России получил новый импульс для развития – президент поставил перед ним задачу к 2024 г. увеличить экспорт сельхозпродукции в два с лишним раза, до \$45 млрд. При этом государство активно поддерживает аграриев в рамках Национальной программы развития АПК и других инициатив. Эта поддержка способствует росту, но для достижения поставленных целей одних только субсидий и квот будет недостаточно – даже если поле засеять деньгами, урожай не вырастет вдвое. Чтобы повысить эффективность сельского хозяйства, нужно переходить на новые методы и технологии – иначе говоря, российскому аграрному сектору жизненно необходима цифровизация.

Реальность и перспективы

Когда речь заходит о том, на каком этапе сейчас находится цифровизация российского сельского хозяйства, цифры огорчают и обнадежи-



вают одновременно. Так, на конференции «Точное земледелие – 2018» Минсельхоз сообщил, что аграрный сектор страны занимает по уровню цифровизации 15-е место в мире, а объем рынка информационно-компьютерных технологий в отрасли составляет около 360 млрд руб. При этом, по данным Росстата, аграрный сектор РФ приносит больше валютной выручки, чем ВПК. Вместе с тем, согласно исследованиям Росстата и экспертным оценкам, рентабельность производства в агросекторе составляет порядка 30%, около 470 тыс. единиц сельхозтехники имеет возраст более 10 лет, а из примерно 4,4 млн работников, занятых в сельском хозяйстве, только 500 тыс. – квалифицированные специалисты.

На фоне этих объективных проблем вырисовываются вполне оптимистичные перспективы – Россия входит в топ-5 стран по темпам цифровизации. Эксперты считают, что цифровые технологии снизят девиацию урожайности как минимум на 10%, а также уменьшат влияние человеческого фактора на эффективность сельскохозяйственного производства. Помимо решения этих задач, цифровизация будет способствовать снижению трудоемкости работ, минимизации капиталовложений и уменьшению вредного воздействия на окружающую среду.

Сначала автоматизация, потом цифровизация

Цифровизация сельского хозяйства невозможна без его автоматизации – это та самая база, без которой нельзя двигаться дальше. Прежде чем задействовать «умные» технологии, собирать и анализировать данные, необходимо свести на нет

негативное влияние человеческого фактора – именно это в первую очередь подразумевается под автоматизацией. Не секрет, что одним из тормозов развития отрасли выступает кадровый вопрос. С одной стороны, здесь играет роль отток населения в города, с другой – привлечению специалистов препятствуют сезонность работы, устаревший подход к организации труда во многих хозяйствах и низкий уровень зарплат. В результате молодежь выбирает для себя другие отрасли, профессионалы стареют, а на работы приходится привлекать неквалифицированный персонал.

В этих условиях автоматизация сельскохозяйственных работ важна как никогда. Это не значит, что на поля должны выйти автоматические трактора и комбайны – операторы по-прежнему нужны, но техника благодаря геолокации, системе параллельного вождения и другим технологиям способна исправлять и предупреждать их ошибки. Кстати говоря, такие машины не только повышают эффективность работы, но и отчасти способствуют решению кадровой проблемы. Одно дело – управлять трактором, выпущенным в прошлом веке, и совсем другое – сесть за руль «умной» техники. Это само по себе мотивирует учиться управлять ею, а за счет того, что выработка на таких машинах гораздо выше, чем при работе по старинке, оператор получает более высокую зарплату.

При этом оператор отнюдь не превращается в бесплатное приложение к машине – он может задавать последовательность действий, «обучать» машину определенному набору операций, которые та потом будет последовательно выполнять.

Когда этот этап пройден, можно говорить о цифровизации, поскольку «умная» техника оснащена сотнями датчиков, собирающих информацию. С их помощью накапливаются всевозможные данные – о температуре и влажности почвы и воздуха, неисправностях самой техники, структуре поля, урожайности и т.п. Затем эта информация передается в единую систему, анализируется и используется в дальнейшей работе. Например, благодаря такому обмену данными можно уменьшить продолжительность простоев из-за неисправностей: ведется постоянный мониторинг машины, и как только поступает сигнал об износе тех или иных деталей, сервисные инженеры выезжают на место и устраняют проблему прежде, чем произойдет сбой.

Дифференцированное земледелие

Предупредить ошибки оператора – далеко не все, на что способны «умные» сельхозмашины, а действия человека – далеко не единственный фактор, влияющий на урожайность. В сельском хозяйстве многое зависит от погодных условий, состояния почвы и т.д. При этом на одном и том же поле могут быть более или менее влажные



участки, лучшее или худшее качество почвы, но обычная техника этого не видит – она просто сеет, поливает или вносит удобрения согласно предписаниям (при условии, что оператор эти предписания выполняет, что случается далеко не всегда).

Совсем другое дело – цифровая техника, которая «видит» эту разницу и определяет интенсивность полива или количество вносимых удобрений на каждом конкретном участке поля. Она позволяет любую сельхозоперацию выполнять дифференцированно, и неважно, будет ли это посев, подкормка или орошение.

Разумеется, трактор или комбайн «замечает» различия на соседних квадратных метрах не сам по себе – для этого он должен быть включен в единую систему, куда поступают данные с датчиков всей техники, метеостанций, беспилотных аппаратов, фотографирующих поля с заданным интервалом и т.п. Это не обязательно должна быть система одного агрохолдинга – напротив, чем шире ее охват, тем больше в ней данных, тем точнее она показывает текущую ситуацию и прогнозирует ее в будущем.

В России подобная система существует – она запущена одним из ведущих производителей сельскохозяйственной техники, но при этом не заточена под машины конкретного производителя. В настоящее время она охватывает более 2,1 млн га (включая Украину и Казахстан), и все больше хозяйств задумываются о подключении к ней. Уже были реализованы первые пилотные проекты с ее использованием, и их результаты весьма обнадеживают. Оценивать их пока рано, но рост урожайности может достигнуть 10–15% при снижении затрат на 20%.

Словом, у российских аграриев есть все, чтобы Национальная программа развития АПК была успешно реализована – в конце концов, в этом заинтересованы и они сами, и государство, и производители техники, и конечные потребители сельхозпродукции, которые могут даже не подозревать, что обычная картошка, попадающая на их стол, качественна, полезна и экологична как раз потому, что выращена по «умным» технологиям. ИКС

Круглогодичный фрикулинг в России, или Готовых рецептов нет

Александра Эрлих, сеньор-консультант, CABERO

Использование испарительных технологий в системах вентиляции российских ЦОДов может обеспечить практически круглогодичный фрикулинг, хотя реализация такой системы потребует детальных расчетов.



Старая школа и современные системы

Поступив в 2002 г. в Билефельдский университет в Германии, я на первых же каникулах прошла практику в компании Schüco, в подразделении, которое занималось солнечными батареями. В начале 2000-х Schüco считалась самым современным и прогрессивным предприятием в Германии в области гелиоэнергетики. Оно и было таковым, за исключением, как ни странно, отдела ИТ. Здесь трудились специалисты, получившие образование в конце 80-х. Они обслуживали компьютеры, работающие под DOS, но не разбирались в более современной Windows и ее приложениях. Вместо того чтобы учиться, программисты старой школы, назовем их так, скупали по всей Германии старые компьютеры, разбирали их на запасные части и ремонтировали устаревшую технику. Сочетание было гротескным: ультрасовременные солнечные батареи и морально устаревшие компьютеры.

Вспомнила об этой истории, столкнувшись недавно с тем, что некоторые «современные» ЦОДы в России до сих пор проектируются на прецизионных кондиционерах без разделения коридоров. Не хочу рассуждать о многочисленных недостатках таких систем, об этом сказано и написано достаточно. Мне, как, надеюсь, и вам, интересны более современные и прогрессивные модели. Их на сегодняшний день много, но в рамках данной статьи хочу остановиться на ЦОДах, в которых снятие тепловыделений от ИТ-оборудования происходит за счет использования систем вентиляции. Точнее, прямооточных систем вентиляции.

Эти системы обладают рядом важных преимуществ:

- относительно низкие инвестиционные затраты;
- низкое (наверное, самое низкое из всех современных систем) энергопотребление;
- простота эксплуатации.

Здесь стоит добавить – «при прочих равных условиях». Что я имею в виду?

Температурно-влажностная проблема...

Натолкнулась недавно в немецкой прессе на кричащую статью о суперсовременном «зеленом» ЦОДе Centron в городе Бамберг. Страница рекламных слоганов о сравнении различных систем и о том, что выбранная ими вентиляционная прямооточная система обеспечивает в течение 95% времени в году бескомпрессорную работу ЦОДа при сохранении температуры в машзале не выше +24°C. Ура! Найдена, наконец, идеальная дешевая система охлаждения дата-центра, и ее можно тиражировать. Увы и ах. Прямоточная система отлично работает в ЦОДе Centron по одной простой причине: максимальная температура воздуха в Бамберге составляет 25,7°C, и наблюдается она всего лишь несколько часов в одном месяце в году, в июле. Все остальное время года температура воздуха в этом славном городе колеблется в интервале от -2,5 до +24°C при среднегодовой температуре +9,5°C (табл. 1).

Здесь мы подошли к первой проблеме использования прямооточной вентиляционной системы в ЦОДе: **температуре**. В Москве, например, температура ниже +24°C бывает около 93% времени – 11 месяцев в году (табл. 2). Для обеспечения микроклимата в дата-центре в оставшиеся 7% времени, когда температура выше +24°C, нужно либо доукомплектовывать систему дополнительным охлаждением, либо поднимать температуру в машзале, если позволяет ИТ-оборудование.

На территории Российской Федерации почти нет мест, обладающих столь же гомогенным климатом, каким обладает добрая половина городов в Германии, включая вышеупомянутый Бамберг. А за Уралом климат и вовсе резко континентальный. Для него характерны большие

Табл. 1.
Климат Бамберга

Показатель	Янв.	Фев.	Март	Апр.	Май	Июнь	Июль	Авг.	Сен.	Окт.	Нояб.	Дек.	Год	
Максимальная средняя температура, °C	4,1	5,5	9,8	15,4	19,8	22,9	25,1	24,5	20,2	14,2	7,1	3,9	Ø	14,4
Минимальная средняя температура, °C	-2,2	-2,5	0,4	3,2	7,3	10,9	13,0	12,2	8,8	5,2	1,2	-1,5	Ø	4,7
Средняя температура, °C	0,9	1,4	4,9	9,3	13,8	17,1	19,0	18,1	14,1	9,3	4,1	1,2	Ø	9,5
Осадки, мм	40	33	39	27	46	52	73	46	46	39	36	38	Σ	515
Число солнечных часов в день	1,6	2,4	3,1	4,5	5,4	6,1	6,0	5,7	4,1	2,7	1,2	1,1	Ø	3,7
Количество дождливых дней	13	12	13	11	10	12	13	10	10	12	13	13	Σ	142
Влажность воздуха, %	85	81	77	72	70	71	71	75	79	83	85	86	Ø	77,9

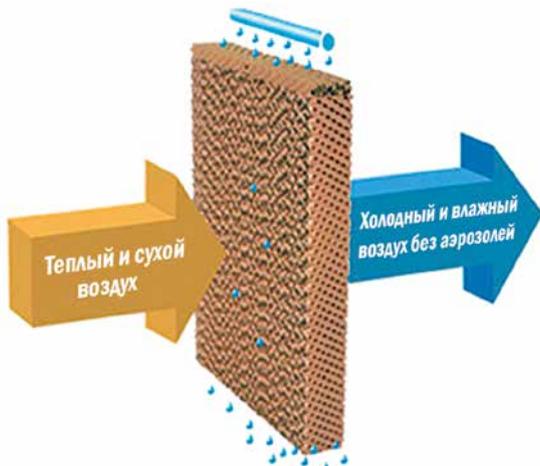
Источник: WetterKontor, Wetterdienst.de

Табл. 2. Климат Москвы ▼

Показатель	Янв.	Фев.	Март	Апр.	Май	Июнь	Июль	Авг.	Сен.	Окт.	Нояб.	Дек.	Год
Абсолютный максимум, °С	8,6	8,3	19,7	28,9	33,2	34,7	38,2	37,3	32,3	24,0	16,2	9,6	38,2
Средний максимум, °С	-4	-3,7	2,6	11,3	18,6	22,0	24,3	21,9	15,7	8,7	0,9	-3	9,6
Средняя температура, °С	-6,5	-6,7	-1	6,7	13,2	17,0	19,2	17,0	11,3	5,6	-1,2	-5,2	5,8
Средний минимум, °С	-9,1	-9,8	-4,4	2,2	7,7	12,1	14,4	12,5	7,4	2,7	-3,3	-7,6	2,1
Абсолютный минимум, °С	-42,1	-38,2	-32,4	-21	-7,5	-2,3	1,3	-1,2	-8,5	-20,3	-32,8	-38,8	-42,1
Норма осадков, мм	52	41	35	37	49	80	85	82	68	71	55	52	707

Рекорды за весь период наблюдений (1879–2016) – объединенные данные ТСХА и ВДНХ, норма (1981–2010) – ВДНХ
 Источник: Погода и Климат

Рис. 1. ▶
 Принципиальная
 схема адиабати-
 ческой системы
 охлаждения
 на основе матов



амплитуды колебаний температур – как годовых, так и суточных (табл. 3).

Относительно невысокая **влажность в холодное время года** – вторая большая проблема при использовании прямоточной вентиляционной системы в ЦОДах.

Не буду подробно останавливаться на том, почему именно влагосодержание в ЦОДе может стать большой проблемой – об этом писала отдельную статью*. Суть в том, что если это не корпоративный ЦОД с серверами, сделанными «под вас», то вам сложно будет игнорировать температуру и влажность в ЦОДе. Так что стоит задуматься о том, как решить температурно-влажностную проблему.

...и ее решения

Итак, что делать, когда для охлаждения используется система прямоточной вентиляции, а температура на улице выше допустимой в ЦОДе? Или, наоборот, температура очень низкая, и воздух для ЦОДа слишком сухой? Ответ, казалось бы, лежит на поверхности: применить адиабатическое увлажнение. Взять готовую систему от любого производителя или создать свою, доморощенную, и вперед. Но все не так просто.

К сожалению, не всякая адиабатическая система даст ожидаемый результат. Сделаем небольшой экскурс в мир адиабатических систем.

Адиабатика с использованием матов

На первый взгляд, все замечательно: устанавливаем маты, поливаем их водой, которую якобы даже не нужно подготавливать, и получаем необходимый эффект охлаждения (рис. 1). При этом еще и экономим электроэнергию.

Сегодня на рынке представлено большое количество подобных систем, включая отечественные, и приобрести их совсем не сложно.

Только вот неподготовленная вода содержит большое количество примесей, которые не оседают на стенках мата. А те, что оседают, забивают и без того небольшие отверстия для прохождения воздуха.

Для достижения эффекта охлаждения в 10 К необходим мат толщиной не менее 300 мм, который создает сопротивление по воздуху не менее 200 Па. Это сопротивление вентиляторы установки должны будут преодолевать, причем кругло-

Табл. 3.
 Климат Якутска ▼

Показатель	Янв.	Фев.	Март	Апр.	Май	Июнь	Июль	Авг.	Сен.	Окт.	Нояб.	Дек.	Год
Абсолютный максимум, °С	-5,8	-2,2	8,3	21,1	31,1	35,1	38,4	35,4	27,0	18,6	3,1	-3,9	38,4
Средний максимум, °С	-35,1	-28,6	-12,3	1,7	13,2	22,4	25,5	21,5	11,5	-3,6	-23,1	-34,3	-3,4
Средняя температура, °С	-38,6	-33,8	-20,1	-4,8	7,5	16,4	19,5	15,2	6,1	-7,8	-27	-37,6	-8,8
Средний минимум, °С	-41,5	-38,2	-27,4	-11,8	1,0	9,3	12,7	8,9	1,2	-12,2	-31	-40,4	-14,1
Абсолютный минимум, °С	-63	-64,4	-54,9	-41	-18,1	-5,4	-1,5	-7,8	-14,2	-40,9	-54,5	-59,8	-64,4
Норма осадков, мм	9	8	7	8	20	35	38	37	31	18	16	10	237

Источник: Погода и Климат

году, что несколько не уменьшит, а, наоборот, увеличит энергопотребление. Затем, как вы помните, на матах осел известковый налет, и сечение отверстий для прохода воздуха уменьшилось вдвое, а то и втрое. До каких величин возрастет сопротивление? Как часто службе эксплуатации придется заниматься заменой матов?

А еще резервирование: придется либо обеспечить второй источник воды, либо предусмотреть баки с необходимым объемом воды на орошение. И не забыть систему обеззараживания воды... И запас матов.... Стоимость такой системы достаточно велика даже без учета частой замены матов.

Что мы там говорили о прецизионниках?

Форсуночная адиабатика без испарения с поверхности

Для такой системы мы подготавливаем воду, но надеемся получить необходимый эффект охлаждения, используя форсунки различной конфигурации (рис. 2).

На рынке огромное количество вариантов, и все обещают необыкновенный эффект. Советую выбирать тех производителей, которые проводят точный доказательный расчет нужного количества форсунок/необходимой воды на орошение.

Кто встречал такие системы в кафе, наверняка отметил, что под ними по ощущениям действительно холоднее. Используя форсуночную адиабатику без испарения с поверхности, можно снизить температуру на 5 К. И встречаются системы, где как раз этих 5 К бывает достаточно. Но, к сожалению, в большинстве случаев 5 К не хватает.

Не говоря уже о том же резервировании, что и в случае адиабатических матов.

У подобных систем есть только одно преимущество: отсутствие дополнительного сопротивления воздухообмену.

Поверхностное испарение

Мы берем теплообменный блок, с его поверхности испаряем воду и достигаем эффекта понижения температуры на 10 К (рис. 3). Так же, как и в предыдущем варианте, нам нужна водоподготовка, пусть и самая простая. Плюс точный расчет требуемой площади поверхности/количества форсунок/необходимой воды на орошение.

В отличие от предыдущего варианта, возникает небольшое сопротивление по воздуху, от 35 Па. Но, в отличие от варианта адиабатических матов, в этих системах сопротивление не увеличивается с количеством часов работы. Да и нагрузка на вентиляторы в пять-шесть раз ниже.

Явное преимущество такой системы – двойная возможность резервирования. Можно, как и в предыдущих вариантах, делать резервирование по воде. А можно организовать систему ре-



Рис. 2. Форсуночная адиабатическая система без испарения с поверхности

зервного охлаждения посредством дополнительного замкнутого холодильного контура.

«Снова холодильный контур? – скажете вы. – Может, сразу прецизионники?» Не важно, что они занимают место в машзале, которое можно было бы заполнить стойками, и потребуют коммуникаций, и энергопотребление вырастет, и есть ограничения по температурам. Но ведь привычно? И не так уж плохо?

Давайте посчитаем

Например, для Москвы максимальная температура влажного термометра, согласно 2017 ASHRAE Handbook – Fundamentals (мы же строим надежный ЦОД!), за последние 20 лет составляет $t_{wb \max} = 24,5^{\circ}\text{C}$. Тот же источник требует расчетов на максимальную температуру воздуха летом (t_{air}), равную $36,8^{\circ}\text{C}$. Целевая температура в холодном коридоре составляет $+24^{\circ}\text{C}$.

При использовании **фреоновой системы** с прецизионными кондиционерами инвестиционные затраты будут относительно невелики, эксплуатация – относительно простой и привычной. И, если у вас достаточно электроэнергии и стоимость ее находится в пределах 1,5–2 руб./кВт, можно остановиться на этой системе и не углубляться в «зеленые» технологии. Главное, не забудьте предусмотреть увлажнение в ЦОДе.

Если же ваша ситуация, как и в большинстве российских ЦОДов, не такова, имеет смысл рас-



Рис. 3. Форсуночная адиабатическая система с поверхностным испарением

смотреть другие системы. Например, все еще оставаясь на **прецизионных кондиционерах**, предусмотреть **фрикулинг**.

Самые современные, и уже довольно дорогие, системы дадут вам фрикулинг максимум от +10°C. Все остальное – пока – находится за пределами разумной экономики.

В климате Москвы фрикулинг будет уверенно работать порядка 5 тыс. ч в году, что само по себе очень хорошо. В этот период не работают компрессоры, лишь вентиляторы драйкулеров вашей установки. Потребление электроэнергии минимальное, и можно получить довольно неплохие среднегодовые показатели PUE, но все же далеко не такие красивые, как при использовании **прямоточной вентиляции с адиабатической системой**.

В этом случае работа в режиме фрикулинга может продолжаться до +24°C наружного воздуха, т.е. примерно 8250 ч в год. Задумайтесь: работа во фрикулинге почти круглый год, малые инвестиционные затраты, дополнительное место в машзале. Электроэнергия расходуется только на работу вентиляторов. Сложности в климате Москвы возникают лишь в оставшиеся 510 ч.

Решение довольно простое, комбинация адиабатики и компрессорного доохлаждения. Почему нельзя использовать только адиабатику?

100%-ное насыщение воздуха невозможно. Иными словами, мы не сможем получить адиабатический эффект при $t_{\text{air}} = t_{\text{wb max}} = 24,5^\circ\text{C}$. Как бы нам ни хотелось, эффект орошения проявится не ранее, чем $t_{\text{wb max}} +$ сопротивление теплообмену = $24,5^\circ\text{C} + 2^\circ\text{C}$ (минимум) = $26,5^\circ\text{C}$.

Назовем эту температуру **нижним порогом орошения**.

Здесь можно пойти несколькими путями:

- Допустить кратковременное повышение температуры в холодном коридоре до +27°C.
- Рассчитывать систему на $t_{\text{wb}} = 19^\circ\text{C}$, утешая себя и заказчика надеждой, что $t_{\text{wb max}} = 24,5^\circ\text{C}$ продержится не более 2% времени в году.
- Предусмотреть дополнительную компрессорную систему «на дожим». Эта система позволит также при необходимости подсушивать воздух.

Именно последний вариант я бы рекомендовал для исключительно надежной работы ЦОДа.

Компрессорная система, работающая на «дожим», будет потреблять гораздо меньше электроэнергии, чем система на прецизионных кондиционерах.

Верхний порог орошения определяется максимальной температурой воздуха и предельными возможностями оросительной системы. Для Москвы при максимальной температуре воздуха $36,8^\circ\text{C}$ возможны следующие комбинации адиабатики и компрессорной системы в прямоточной системе вентиляции:

- Адиабатика с использованием матов охлаждает воздух до $26,8^\circ\text{C}$, далее до 24°C – «дожим» компрессорной системой. Помимо всех недостатков использования матов мы дополнительно увеличиваем сопротивление по воздуху (а, значит, потребление вентиляторов) за счет наличия блоков охлаждения компрессорной системы.

- Форсуночная адиабатика без испарения с поверхности охлаждает воздух до $31,8^\circ\text{C}$, далее до 24°C – «дожим» компрессорной системой. Большая нагрузка на компрессоры, что эквивалентно большему расходу электроэнергии, плюс дополнительное увеличение сопротивления по воздуху (а значит, энергопотребления вентиляторов) за счет наличия блоков охлаждения компрессорной системы.

- Поверхностное испарение охлаждает воздух до $26,8^\circ\text{C}$, далее до 24°C – «дожим» компрессорной системой. При этом не создается дополнительного сопротивления по воздуху, поскольку в качестве блоков системы компрессорного охлаждения используются те же блоки, что и для поверхностного испарения.

Таким образом, из всех систем адиабатического орошения в прямоточной вентиляции для данной задачи самым эффективным оказывается испарение с поверхности. В том случае, если вы остановили свой выбор на прямоточной вентиляции с адиабатической системой.

И это еще не все

Нужно отметить, что в реальном ЦОДе на выбор системы охлаждения влияет гораздо большее количество факторов, чем можно было рассмотреть в рамках этой статьи: геометрия ЦОДа, бюджет, наличие отдельных ресурсов и пр. Их нельзя недооценивать, и каждый вносит свои коррективы в выбор решения. Именно поэтому я не устаю подчеркивать: готовых рецептов климатизации ЦОДа нет. Вам придется заказать индивидуальный костюм. Да, это означает примерки, притирки, разработку индивидуальной концепции, крой, снова примерки. Гораздо сложнее и кропотливее, чем просто использовать готовое стандартное изделие. Со стандартным проще: один раз сходил на рынок, примерил несколько готовых моделей, выбрал наиболее подходящий костюм. И все. Неважно, что там чуть тянет, тут слегка длинноват, тут недоразмерен и не подчеркивает всех ваших достоинств. Главное – быстро.

Но представьте, как будет хорош в эксплуатации индивидуальный, именно по вашему ЦОДу скроенный костюм. Как замечательно будет себя чувствовать ЦОД после того, как костюм будет готов, как комфортно будет в нем и с ним работать. И как привлекательно вы будете выглядеть в глазах клиентов. Поверьте, вам не будет жаль потраченного на индивидуальное решение времени. **ИКС**



Пожаротушение в ЦОДе

Откажитесь от штампов

Современные технологии позволяют остановить пожар в дата-центре в момент его возникновения, когда ущерб от него практически равен нулю. Но, стремясь к сверххранёму обнаружению пожара, мы рискуем часто получать ложные сигналы, а реагируя позже, можно упустить ситуацию из-под контроля... Какие решения позволяют найти компромисс?

Пожары в дата-центрах чреваты огромным прямым ущербом, связанным с потерей данных и дорогостоящего ИТ-оборудования. Но не только. Вследствие пожара в крупном дата-центре в Азербайджане в 2017 г. почти на 7 ч население целой страны потеряло доступ в интернет – зайти в Сеть можно было только с мобильных устройств¹. Есть данные о сбоях в работе устройств Samsung (в основном «умных» телевизоров) в апреле 2014 г., которые могли быть связаны с произошедшим в тот же день² пожаром в дата-центре в южнокорейском Квачхоне. После пожара, случившегося в 2013 г. в дата-центре округа Макомб (шт. Мичиган, США), главе округа пришлось объявить чрезвычайное положение – был потерян доступ к ресурсам муниципального управления и базе данных государственных услуг, даже телефонная связь в офисе главы округа была отключена на несколько дней³. Пожар в дата-центре Shaw Communications Facility в Калгари (Канада) в 2012 г. привел к отключению сервисов многих государственных услуг и вызвал задержки сотен плановых операций в местных больницах⁴.

Когда тушить пожар?

Чтобы избежать тяжелых последствий, нужно трезво и практично готовиться к возможности пожара – правильно проектировать, строить и эксплуатировать дата-центры, оснащая их современными системами противопожарной защиты с учетом не только нормативных требова-

ний, но и закономерностей развития и тушения реальных пожаров.

У специалистов по пожарной тактике есть поговорка: «Любой пожар можно потушить одной ложкой воды, если знать куда, а главное – когда ее вылить». Действительно, возгорание обычно начинается с аварийной ситуации – короткого замыкания, разогрева платы, перегрузки кабельной линии. Температура растет, изоляция перегревается, начинается пиролиз пластика или резины – появляется дымок, за ним тление... этот процесс нарастает медленно, и важно, что в самом начале он невелик по масштабам. Если в этот процесс не вмешаться, тление переходит в открытое горение, и оно начинает бесконтрольно усиливаться.

Пламя распространяется путем прогрева окружающих горючих материалов с их последующим воспламенением. Следовательно, чем больше очаг пожара, тем больше тепла он выделяет – и тем быстрее растет.

Понятно, что проще всего ликвидировать пожар в первые минуты его развития, когда площадь очага пожара, его тепловыделение и скорость распространения минимальны. Недаром в учебниках по пожарной тактике большое внимание уделяется скорости сборов и выезда пожарных подразделений по тревоге, скорости боевого развертывания и проведения разведки – это позволяет «перехватить» возгорание тогда, когда справиться с ним легче всего.

Теоретически оптимальным временем для вмешательства является период до фактического

Василий Углов,
технический директор,
Marioff Russia

¹ <https://www.datacenterdynamics.com/critical-environment/data-center-fire-kills-internet-in-azerbaijan/95227.article>.

² <https://www.cbsnews.com/news/report-samsung-fire-caused-outages-on-devices-smart-tvs>.

³ <https://www.datacenterknowledge.com/archives/2013/04/19/michigan-county-offline-after-data-center-fire>.

⁴ <https://www.datacenterknowledge.com/archives/2012/07/16/data-center-fire-disrupts-calgary>.

начала горения. Если знать, где в следующую минуту воспламенится кабель, то предотвратить пожар будет легче: отключить нужный сервер или плату, обесточить кабельную линию – вылить в нужное место ту самую «ложку воды», – и пожар не возникнет.

И благодаря современным технологиям теперь есть такая возможность! Применение высокочувствительных адресных установок пожарной сигнализации, в частности аспирационного типа, позволяет дать сигнал тревоги даже до появления видимого дыма, в момент начала выделения продуктов термического разложения изоляции перегретых кабелей. Если персонал дата-центра быстро и четко среагирует на сигнал, то можно успеть вживую полюбоваться на начало процесса тления перегретого кабеля – и принять нужные меры, предотвратив возгорание.

Но пожар ли это?

Можно подумать, что автоматизация этого процесса устранил ненадежность «человеческого фактора» и повысит безопасность... Но не все так просто. Чем чувствительнее пожарный датчик, тем раньше он обнаруживает пожар, но тем больше вероятность ложного срабатывания. Причинами «ложняков» могут быть запыленность, химические загрязнения, электромагнитные поля – избавиться от рисков ложного срабатывания нельзя. Специальные средства борьбы с ложными срабатываниями (как аппаратные, так и программные) существуют и с успехом применяются – но, как правило, они приводят к загромождению чувствительности датчиков и замедляют обнаружение пожара. Или мы «ловим» пожар рано, но рискуем часто получать ложные сигналы, или обнаруживаем пожар очень достоверно, но на более поздних стадиях.

Если на сигнал о пожаре реагируют люди, то ложные срабатывания не являются большой проблемой. Быстро выяснить, что именно происходит в конкретной электрощитовой или серверном шкафу, нетрудно для хорошо обученного сотрудника. Но если на пожар реагирует автоматическая установка пожаротушения, все становится сложнее.

Традиционно дата-центры защищаются автоматическими установками газового пожаротушения (АУГП). Современные газовые составы – эффективное средство, безопасное для деликатного оборудования дата-центров.

Но АУГП дороги, и, что самое важное, большая часть их стоимости – это стоимость газа. При получении сигнала о пожаре установка пожаротушения не открывает подачу газа сразу, а обеспечивает задержку срабатывания для проведения эвакуации, и уже потом заполняет помещение газом. Это значит, что персонал дата-центра в случае пожарной тревоги в первую очередь покидает защищаемые помещения, следит за тем, чтобы двери после эвакуации были плотно закрыты (чтобы газ не улетучился из защищаемого объема), и после этого вызывает пожарную охрану, сотрудники которой в изолирующих противогазах должны проникнуть в горящее помещение и выяснить, что, собственно, в нем происходит.

Поэтому, когда пожарная сигнализация выдает сигнал «Пожар!», собственник объекта в первую очередь... платит миллионы рублей за перезарядку установки пожаро-

тушения, поскольку выпущенный газ нельзя опять собрать в баллоны. И только после срабатывания АУГП можно, наконец, начать выяснять, ложное ли это срабатывание или реальное возгорание. С точки зрения служб эксплуатации приемлемым решением было бы эксплуатировать установки газового пожаротушения только в ручном режиме, отключив автоматику, но это впрямую запрещено нормативами.

Казалось бы, когда чувствительные датчики сообщили о пожаре, у нас есть несколько драгоценных минут, чтобы прибыть на место тревоги, выяснить, что происходит, и элементарными действиями предотвратить беду, но персонал обязан срочно эвакуироваться из помещения.

А если тушить водой?

Возможны и другие решения. Установки пожаротушения тонкораспыленной водой (АУП ТРВ) используют, как следует из их названия, чистую воду. Эффективность воды в полной мере проявляется при распылении ее в виде струй водяного тумана – они перемешивают пламя, насыщают его парами воды, снижают температуру в зоне горения, осаждают дым и защищают от прогрева окружающее оборудование. Тонкая водяная пыль, висящая в воздухе, поглощает тепловое излучение, не давая пожару распространяться. Ущерб от воздействия воды на оборудование минимален – водяная пыль, оседающая на поверхностях, накапливается медленно. При этом чистая вода обладает важным преимуществом – она безопасна для людей. Этот очевидный факт означает, что срабатывание АУП ТРВ не требует эвакуации персонала и не может помешать ему предпринять срочные действия непосредственно на месте возникновения аварийной ситуации.

А как быть с ложными срабатываниями? Распылять воду – пусть и в виде тонкого тумана – на работающие серверы в том случае, если пожара, может быть, и нет вовсе – это не выглядит безопасным решением.

Именно поэтому для АУП ТРВ давно разработаны и успешно применяются спринклерно-дренчерные узлы управления, позволяющие осуществлять двойной контроль срабатывания. Трубопроводная сеть АУП ТРВ в этом случае делится на водозаполненную (от насосной установки до узла управления) и сухотрубную части (от узла управления до распылителей, расположенных в защищаемом помещении). Распылители в таких установках применяются спринклерные, нормально закрытого типа, оснащенные термочувствительной колбой, которая лопается при достижении определенной температуры. Сухотрубная часть в дежурном режиме заполнена воздухом под давлением – закрытые колбы распылители не дают давлению воздуха упасть, а закрытый узел управления держит воду, не давая ей поступать в секцию трубопровода, расположенную в защищаемом помещении.

При получении сигнала «Пожар!» от пожарной сигнализации узел управления открывает подачу воды в трубопровод, но вода не распыляется через оросители, если их термочувствительные колбы не лопнули; и только когда температура достигнет нужного значения, спринклеры открываются и начинают тушить пожар.



Такая технология позволяет отсечь ложные срабатывания, обеспечивая пожарной сигнализации возможность предупреждать о пожаре на сверхранней стадии и при этом начинать тушение только в той ситуации, когда пожар действительно начал развиваться. При случайном разрушении колбы спринклера падение давления воздуха в трубопроводе сигнализирует об этом, но вода на тушение подаваться не будет, поскольку нет сигнала от пожарных датчиков.

Но мы же помним, что тушить пожар эффективнее всего в момент его начала, когда ущерб от него еще равен нулю, а для тушения достаточно минимальных затрат? Можем ли мы ждать, пока колба распылителя прогреется, чтобы начать тушение?

Оптимальный сценарий

Здесь на первый план выходит безопасность тонкораспыленной воды для персонала. АУП ТРВ не требуют эвакуации людей при срабатывании, что позволяет сотрудникам отработать полный цикл действий при получении сигнала «Пожар!»: прибыть на место происшествия, осмотреть оборудование и проанализировать ситуацию, отключить кабельные линии, произвести переключение на резервное оборудование – осуществить вмешательство в нужный момент и с хирургической точностью, не допуская перерастания возгорания в полномасштабный пожар.

Если же действия персонала успехом не увенчаются, горение выйдет из-под контроля и начнет распространяться, то вот на этой стадии спринклеры, прогревшись, начнут распылять водяную пыль. Таким образом, АУП ТРВ выступает в качестве последней линии обороны, блокируя развитие пожара, когда люди не смогли справиться с ним быстро и эффективно, и консервируя ситуацию до прибытия пожарных подразделений. При этом снижение температуры и осаждение дыма, вызванные распылением воды, не только защищают оборудование и конструкции дата-центра, но и обеспечивают безопасные условия для эвакуации персонала (на этой стадии ее уже нужно проводить) и улучшают условия работы пожарных, которые по прибытии должны взять ситуацию под свой контроль.

Следует также отметить, что АУП ТРВ, в отличие от установок газового пожаротушения, не требуют герметичности помещения. Будет ли дверь в машзал закрыта после эвакуации или останется распахнутой – тонкораспыленная вода будет работать одинаково эффективно.

Таким образом, можно разработать систему противопожарной защиты объекта, которая будет оптимально совмещать подсистемы обнаружения и автоматического тушения пожара с организационными мероприятиями, позволяющими обученному персоналу эффективно действовать для минимизации возможного ущерба как в случае реального возгорания, так и в случае ложных срабатываний автоматики.

На практике удастся обеспечить:

- применение высокочувствительных датчиков пожарной сигнализации, обнаруживающих пожар на ранней стадии;
- условия для безопасной работы персонала по ликвидации аварийной ситуации в первые минуты ее развития, когда это наиболее эффективно;
- защиту оборудования дата-центра от ложных срабатываний пожарной автоматики, сведение к нулю затрат на ликвидацию последствий «ложняков»;
- эффективную локализацию и тушение пожара, если остановить возгорание вручную не удалось.

Сочетание квалифицированного персонала, высокочувствительных аспирационных установок сигнализации и надежных систем пожаротушения тонкораспыленной водой высокого давления позволяет минимизировать риски ущерба при самых разных сценариях развития аварийных ситуаций. Это не означает, что такое решение всегда будет оптимальным – в пожарном деле не бывает универсальных решений; важно иметь в арсенале широкий спектр технологий и комбинировать их, анализируя реалистичные сценарии развития событий.

Все, что для этого нужно, – начать мыслить за пределами традиционных решений, не бояться анализировать аварийные сценарии и готовиться к ним и не рассматривать пожарную безопасность как необходимость формально выполнять предписания нормативных документов максимально дешевым способом. **ИКС**

PFM задают тренд

Александр Барсков

ЦОДов сегодня требуется все больше, строить их надо все быстрее и при этом обеспечивать высокое качество и адаптивность к зачастую непредсказуемо меняющейся ситуации. Добиться этого можно с помощью модульных решений высокой заводской готовности (PFM).

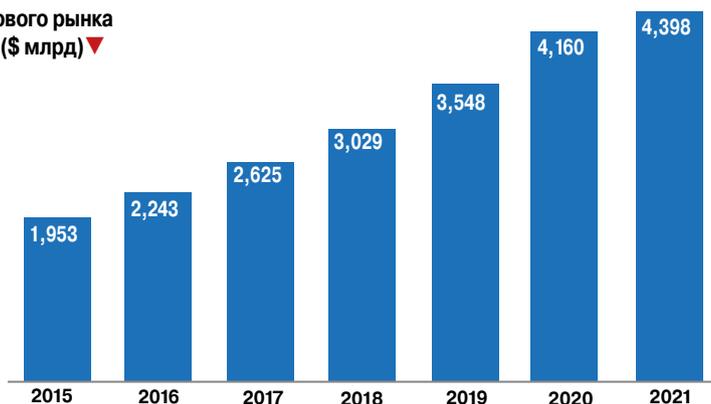
Неудивительно, что именно решения PFM (pre-fabricated modules) оказались в центре внимания конференции Data Center Design and Engineering – 2019, организованной «ИКС-Медиа».

Когда важна скорость

Продукт PFM может представлять собой полностью готовый ЦОД, например, на одну или несколько стоек, с предустановленными на заводе инженерными системами (ИБП, кондиционером, PDU, средствами пожарной безопасности и пр.). В некоторых вариантах модули-ЦОДы стыкуются друг с другом, формируя объекты с десятками, сотнями и даже тысячами стоек. В крупных дата-центрах часто используют модули PFM, реализующие одну из основных инженерных систем, скажем, электропитания или охлаждения. Такие модули подсоединяются к ЦОДу (традиционному или модульному), добавляя необходимые ему ресурсы: электропитания, охлаждения, площади для размещения оборудования.

Согласно данным 451 Research, в 2018 г. объем мирового рынка PFM-решений превысил \$3 млрд (рис. 1). К 2021 г. он увеличится до \$4,4 млрд, а средний ежегодный темп роста в 2015–2021 гг. составит 14,4%. Рынок этот, как считают аналитики, характеризуется значительным конкурентным давлением.

Рис. 1. Объем мирового рынка PFM (\$ млрд) ▼



Источник: 451 Research, 2018 г.

Рынок модульных решений для ЦОДов стал настолько заметным, что эксперты Uptime Institute даже разработали специальную программу Tier Ready для упрощения сертификации объектов, построенных на базе таких решений.

Ряд производителей уже получили сертификат Tier Ready. Так, Huawei предложила модульный ЦОД Fusionmodule2000 (рис. 2), который стал первым в мире продуктом, имеющим сертификат Tier IV Ready. Это комплексное решение представляет собой оснащенный всеми необходимыми инженерными системами модуль для размещения ИТ-нагрузки мощностью до 128 кВт (в варианте с интегрированным ИБП). При размещении ИБП снаружи модуля мощность ИТ-нагрузки можно увеличить до 145 кВт, а при выносе и блока распределения – до 235 кВт. Для создания серверных и небольших ЦОДов компания выпускает модули меньших размеров – Fusionmodule800 – на 1–8 стоек.

Решение с сертификатом Tier IV Ready есть и у компании Vertiv, но оно пока не поставляется в регион EMEA, к которому относится Россия. В целом компания предлагает, пожалуй, один из наиболее полных наборов модульных ЦОДов. Он начинается с продукта Vertiv Smart Cabinet (рис. 3). Этот ЦОД размером со стойку оснащен средствами Trellis Critical Insight для мониторинга и удаленного управления, что особенно важно для заказчиков, эксплуатирующих распределенную сеть edge-ЦОДов.

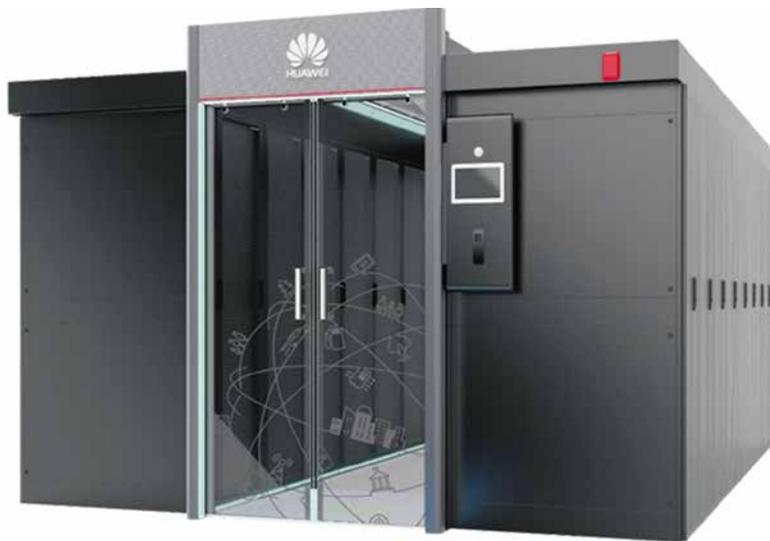
В диапазоне от двух до 12 стоек Vertiv выпускает 11 типовых решений SmartMod. Как отмечает Евгений Журавлев, отвечающий в московском офисе Vertiv за решения для коммерческих ЦОДов (Colo & Cloud), наличие массовых однотипных решений обеспечивает доступные цены, а широкий ассортимент – возможность подбора под особенности конкретного проекта.

При потребности в большем числе стоек Vertiv предлагает объединять модули SmartMod (решение SmartMod MAX), а также выносить модуль электропитания. Такой подход дает возможность разместить уже до 26 стоек. Наконец,



Рис. 2.
Модульный ЦОД
Huawei Fusion-
module2000

Рис. 3.
ЦОД в стойке
Vertiv Smart
Cabinet



имеется вариант SmartMod Hybrid Solution, который позволяет использовать любое оборудование Vertiv и делать инвестиции поэтапно вместе с ростом нагрузки ЦОДа.

Модульные ЦОДы выпускают все основные поставщики комплексных решений для инженерной инфраструктуры ЦОДов. Пожалуй, наибольший опыт в этой области имеет компания Schneider Electric. В частности, для реализации edge-узлов она предлагает не только микро-ЦОДы размером в одну стойку, но и совсем крохотные наноЦОДы. И в то, и в другое семейство входят решения как для офисной инсталляции, так и для размещения в жестких промышленных условиях (рис. 4).

Подход Rittal – разработка edge-ЦОДов с учетом специфики конкретных отраслей и применений. Так, решения для здравоохранения и финансового сектора отличаются усиленной защитой персональных данных и физической защитой, для промышленных ЦОДов обеспечена возможность размещения «в любом месте, где необходимо», вариант для ритейла предусматривает легкое структурирование и работу с различными удельными нагрузками и т.п.

Модульные ЦОДы предлагает и ряд отечественных компаний. На DCDE-2019 такие решения представили, в частности, C3 Solutions и «Импульс». МикроЦОДы DC Vox от C3 Solutions могут быть реализованы на базе одного шкафа или в виде модульной конструкции со стыкующимися шкафами. При выполнении микроЦОДа в одном шкафу он оснащается внутренним блоком кондиционера, в качестве альтернативного варианта можно использовать боковые конди-

ционеры. Для обеспечения бесперебойного электропитания размещенной в микроЦОДе ИТ-нагрузки устанавливаются два ИБП мощностью 10 кВА. Предлагаемые компанией «Импульс» ЦОДы «Итегра» состоят из силового кабинета и необходимого числа ИТ-кабинетов и рядных кондиционеров (рис. 5).

Рис. 5. ЦОДы «Итегра» состоят из силового кабинета и необходимого числа ИТ-кабинетов и рядных кондиционеров

Охлаждение: в поисках оптимального варианта

Производители инженерных систем от продвижения отдельных продуктов все чаще переходят к комплексному анализу всех возможных вариантов, дабы заказчик мог получить действительно оптимальное для своего проекта решение. Так, компания Rittal проанализировала восемь наиболее популярных вариантов систем охлаждения:

- четыре системы на базе чиллеров с турбо- и scroll-компрессорами. Для каждого типа чиллеров рассматривались варианты с внутрирядными кондиционерами и кондиционерами масштаба зала (CRAN);
- три системы на базе фреоновых кондиционеров (DX): шкафных, внутрирядных и внутрирядных с фрикулингом;
- система с непрямым адиабатическим охлаждением.

Анализ проводился в предположении, что ЦОД с инфраструктурой, отвечающей требованиям Tier III, расположен в Москве и имеет ИТ-нагрузку 250 кВт (32 шкафа с удельной нагрузкой 7,81 кВт на шкаф). Для расчетов стоимость 1 кВт·ч электроэнергии принималась равной 4,36 руб. (примерно 0,06 евро).

По капитальным затратам самым выгодным предсказуемо оказалось решение на базе шкафных кондиционеров (рис. 6). Самым дорогим – чиллеры с турбокомпрессорами и внутрирядные кондиционеры. Наиболее энергоэффектив-



▲ Рис. 4. Офисные (вверху) и промышленные наноЦОДы Schneider Electric

ное решение (с рPUE в районе 1,05) – система на основе адиабатики, самое неэффективное (рPUE равно 1,2 и более), оно же самое дешевое – шкафные кондиционеры.

Что касается операционных расходов, рассчитанных на 10 лет, то здесь различия не столь велики, как в показателе рPUE. Наименьшие расходы понесут владельцы систем на основе адиабатики и чиллеров с турбокомпрессорами (рис. 7). Наибольшие – те, кто решит сэкономить на покупке и приобрести фреоновые решения. При этом и рPUE, и OPEX, и TCO зависят от уровня загрузки: эксперты Rittal проанализировали три основных уровня – 50, 75 и 100%.

А вот по общей стоимости владения за 10 лет именно фреоновый вариант – на базе шкафных кондиционеров – оказался самым выгодным (при типичной ИТ-нагрузке 50%). Самый же высокий TCO при указанном уровне нагрузки – у решения на базе чиллеров с турбокомпрессорами и внутрирядных кондиционеров (рис. 8). Интересно, что при эксплуатации со 100%-ной ИТ-нагрузкой один из наименьших TCO оказался у адиабатического решения, которое при 50%-ной нагрузке далеко не самое выгодное.

Разброс значений TCO для большинства рассмотренных вариантов не очень велик. Поэтому

при других начальных условиях (специфика проекта, регион строительства, стоимость ресурсов и пр.) места в этом своеобразном рейтинге могут поменяться. Важно также, подчеркивает Кирилл Дмитриев, ведущий менеджер по продукции «Системы контроля микроклимата» компании Rittal, что ни капитальные, ни эксплуатационные расходы по отдельности не характеризуют систему в целом. На оправданность применения энергоэффективных систем во многом влияют проектная и фактическая ИТ-нагрузки и стоимость ресурсов в регионе.

Выбор системы охлаждения, конечно, зависит еще и от размера объекта. То, что оптимально для ЦОДа на несколько десятков стоек, может плохо подходить для площадки на тысячи стоек. Так, по словам Тобиаса Фокке, директора по продажам в Азиатско-Тихоокеанском регионе компании Stulz, спецификой гиперЦОДов является высокая тепловая нагрузка, нередко уникальная конструкция стоек, отсутствие фальшпола, высокие требования к отказоустойчивости и масштабируемости. Традиционные системы охлаждения для таких объектов далеко не оптимальны, а поставщикам часто приходится подгонять свои решения под конкретный объект/заказчика.

Наилучшим решением для гиперЦОДов специалист Stulz считает кастомизированные блоки охлаждения воздуха (АНУ), которые, как большие кубики, формируют единую стену охлаждения внутри ЦОДа (рис. 9). Такое решение обеспечивает максимальную плотность охлаждения и позволяет также по максимуму использовать пространство в ЦОДе для размещения ИТ-оборудования.

При этом для охлаждения потоков воздуха, проходящих через блоки АНУ, могут использоваться различные технологии, уже рассмотренные выше: охлажденная чиллерами вода, прямое и непрямо испарительное охлаждение, а также фреоновые решения, в том числе в комбинации с системами фрикулинга. Предлагаемые Stulz блоки АНУ имеют типовые размеры, что сокращает время изготовления и доставки, а индивидуальные особенности ЦОДа учитываются благодаря возможности выбора варианта компоновки кубиков в единую систему. Такое решение, помимо прочего, отличается низким уровнем шума и удобством обслуживания, а поскольку располагается вдоль стены серверного зала, то отлично подходит, даже если в зале установлены стойки нестандартных размеров.

Задачи, стоящие перед системами охлаждения, будут только усложняться по мере повышения плотности размещения ИТ-нагрузки. А это практически неизбежно с учетом желания заказчиков максимально эффективно использо-

вать дорогостоящие площади серверных залов, а также очень ограниченное пространство edge-ЦОДов. Именно поэтому Ральф Пленес, вице-президент по продажам и операционной деятельности Raritan и Servertech в странах Европы, Ближнего Востока и Африки (ГК Legrand), предлагает для повышения плотности мощности постепенно увеличивать высоту серверных стоек с 41 до 52U. Следующий шаг, по его мнению, – переход на новые конструктивы высотой 62U.

В таких стойках будут предусмотрены более удобные средства для организации кабельного хозяйства, а вверху – специальное место для установки коммутаторов ToR (рис. 10). Для подобных стоек будут выпускаться и новые интеллектуальные блоки PDU длиной до 2,5 м.

Электропитание: отход от традиций

Если для организации охлаждения ИТ-нагрузки существует множество разнообразных технологий, то для обеспечения бесперебойного гарантированного электропитания выбор существенно меньше. Многие годы, даже десятилетия, основным для ЦОДов являлся вариант на базе статических ИБП и дизель-генераторных установок. Лет пять-семь назад в ЦОДах стали активно применяться динамические ИБП, однако задействовать их целесообразно начиная с мегаваттных мощностей. Но ситуация меняется.

Например, компания Piller предлагает ДИБП CRM300, один модуль которого рассчитан на 300 кВт. Это безбатарейные ИБП, в которых в качестве источника автономной электроэнергии используется маховик Powerbridge PB6, способный «держат» нагрузку 300 кВт в течение 20 с. В параллель можно устанавливать до восьми модулей CRM300, что позволяет формировать си-

стему мощностью до 2,4 МВт. Как утверждает Владислав Ротань, директор по развитию бизнеса компании Piller в России, замена подшипников в CRM300 осуществляется один раз в 11 лет, а стоимость такой замены – 7 тыс. евро.

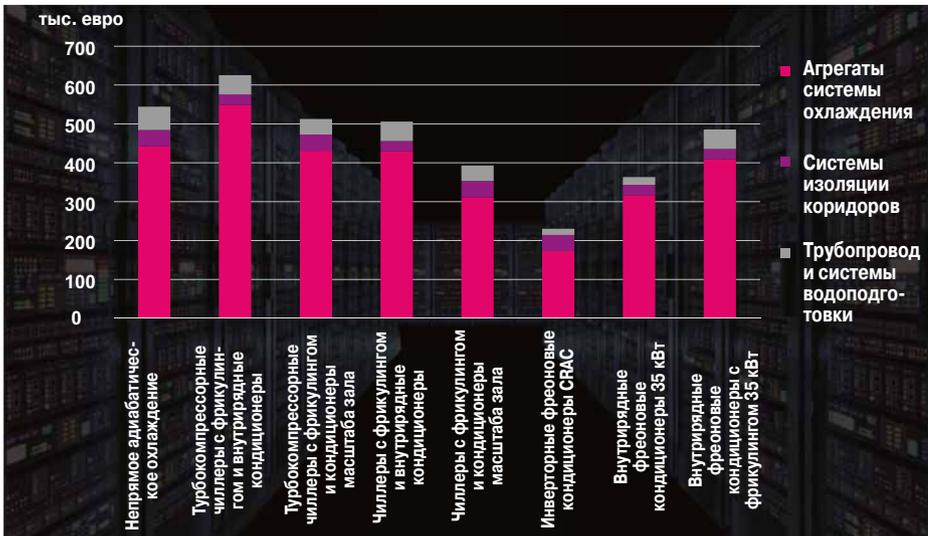
В CRM300 применяется относительно небольшой маховик, но в арсенале Piller есть и гигант – PB60+, способный целую минуту питать нагрузку в 1 МВт. Интересно и предлагаемое Piller решение IP-Bus, которое позволяет строить ЦОДы Tier IV по схеме резервирования не 2N, а N + 1, что сокращает число необходимых элементов, а значит, и расходы заказчика (подробнее см. «ИКС» № 3'2019, с. 62). Всего в мире компанией установлено более 45 систем IP-Bus, есть ЦОД, сертифицированный на Tier IV. В России соответствующий вариант прорабатывается с одним из заказчиков.

Если говорить об экономическом сравнении двух основных вариантов (динамические и статические ИБП), то, как признает В. Ротань, «в пересчете на 1 кВт наши динамические решения на 15–20% дороже обычных статических». Но в таких сравнениях не учитывают полную стоимость энергоцентра, включая стоимость самого помещения необходимой площади, питающих трансформаторов и ВРУ, распределительной системы, систем кондиционирования и вентиляции. «Просчитав более 100 проектов, могу сказать, что при мощности 3–4 МВт полная стоимость энергоцентра с ДИБП не превысит стоимость решения на базе статических ИБП, – заявляет В. Ротань. – Требуется примерно на 50% меньше площади, не нужно кондиционирования, на 30–40% ниже стоимость распределительной системы и соответствующих монтажных работ».

Что касается эксплуатационных расходов, то здесь динамические ИБП, как считает их поставщик, однозначно выигрывают – в первую оче-

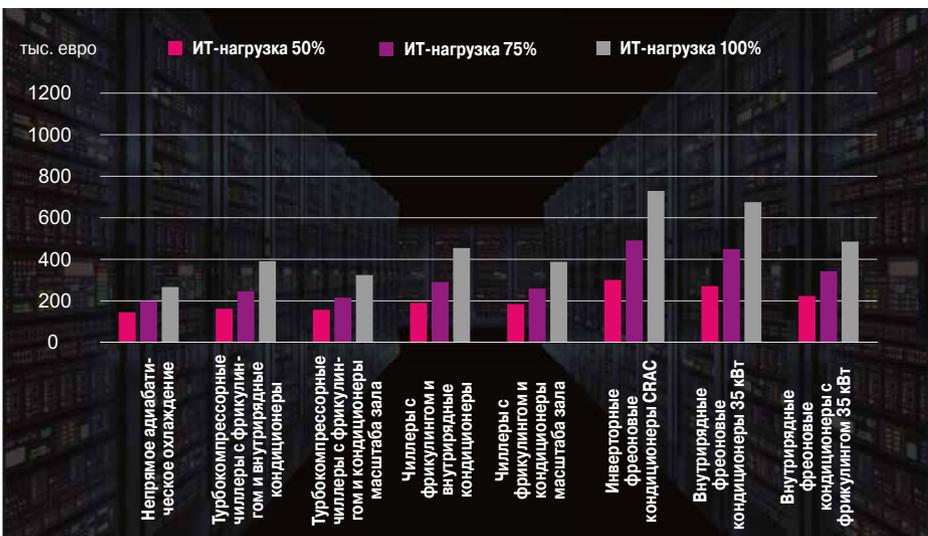


Рис. 5.
Модульные ЦОДы
отечественной
компании
«Импульс»



▲ Рис. 6. Оценка CAPEX различных систем охлаждения

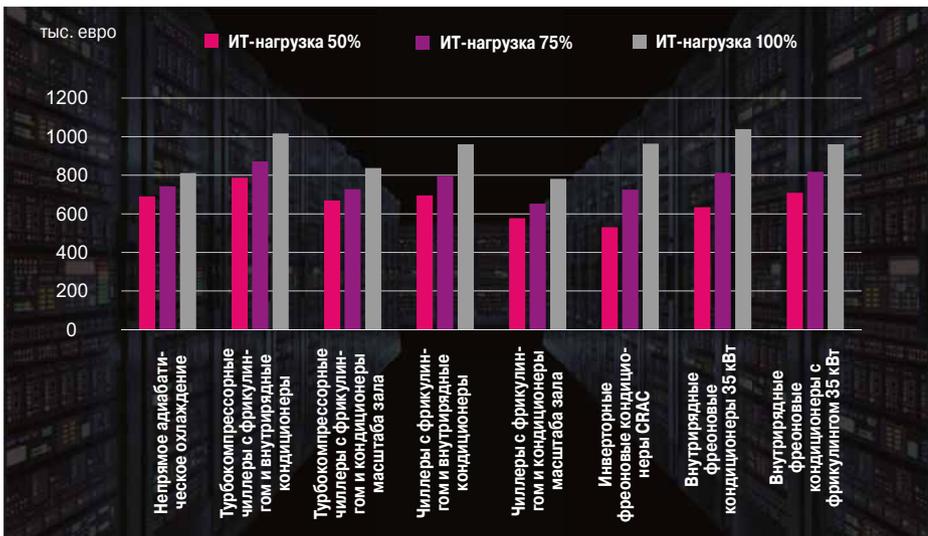
Источник: Rittal



▲ Рис. 7. Оценка OPEX за 10 лет в зависимости от ИТ-нагрузки для различных систем охлаждения

Источник: Rittal

▼ Рис. 8. Оценка TCO за 10 лет в зависимости от ИТ-нагрузки для различных систем охлаждения



Источник: Rittal

редь благодаря снижению потребления электроэнергии и отсутствию необходимости замены АКБ (ввиду их отсутствия как таковых). «К сожалению, только 5% российских заказчиков выбирают решение с учетом TCO», – посетовал представитель Piller.

Если раньше поставщики статических ИБП, похоже, не воспринимали ДИБП всерьез, то сейчас они все чаще отвечают на «угрозы» со стороны конкурентов. Например, таким ответом со стороны компании Vertiv стала разработка продуктов Trinegy Cube и Liebert EXL S1. Как утверждает Е. Журавлев, эти решения сравнимы с ДИБП по стоимости обслуживания и имеют меньшую стоимость владения (за счет существенной экономии на потерях электроэнергии). При использовании литий-ионных АКБ площадь, занимаемая решениями на базе этих ИБП, сравнима с площадью ДИБП, а при использовании АКБ VRLA (7–8 мин автономии) – всего на 10–15% больше. КПД новых ИБП, подчеркивает Е. Журавлев, в режиме VFI выше 96,3% в диапазоне нагрузки от 25 до 100%; а в стандартном для ДИБП режиме VI – превышает 98% в диапазоне нагрузки 20–100%. Наконец, новинки совместимы с маховиками (Vycon).

Существенно снизить OPEX можно и за счет использования в качестве источников электричества и холода турбодетандерных установок, которые на DCDE-2019 представили специалисты компании «Пульсар». Суть технологии – получение энергии и холода при сбросе давления магистрального газа (для доставки его потребителям) на газовых редуционных станциях и пунктах. Поступающий под высоким давлением из магистрали газ вращает турбину, которая, в свою очередь, раскручивает вал ротора генератора – вырабатываемая генератором электроэнергия направляется потребителям. При расширении газа его температура снижается, «бросовый» холод можно утилизировать по традиционным схемам, применяемым в ЦОДах.

Когда говорят о простоях ЦОДов в связи с электропитанием, то, как правило, рассматривают перебои во



Рис. 9. Блоки АНУ, как большие кубики, формируют единую стену охлаждения внутри ЦОДа

Рис. 10. Стойки высотой 62U



внешней электросети. Однако и внутри электросистемы ЦОДов есть немало опасностей. Одна из них – возникновение электродуги, которая может приводить не только к разрушению распределительного щита, но и к повреждениям другого оборудования, травмам и даже гибели сотрудников дата-центра. Причин возникновения электродуги множество: это и ошибки во время переключений либо ремонтных работ, перенапряжения, возникающие при коммутационном процессе, грозовые перенапряжения, попадание инородных тел в изоляционные промежутки, плохие контактные соединения.

Сложность борьбы с электродугой, как отмечает Михаил Саликов, директор по продажам в России и Казахстане компании Eaton, заключается в том, что она развивается очень быстро, защитный автомат не успевает сработать. Для защиты от возникновения электродуги компания Eaton разработала комплекс ARCON, состоящий из датчиков и короткозамыкателя. Электродуга характеризуется интенсивным испусканием света и изменением силы тока. Датчики распознают эти признаки, а короткозамыкатель быстро «гасит» дугу, затем происходит отключение с помощью автоматов. При этом сохраняется все оборудование щита, заменить надо будет только короткозамыкатель.

Другая опасность, на которую обращает внимание М. Саликов, связана с перегревом щитового оборудования. Контроль температуры в щите вручную требует значительных трудозатрат, при этом создаются дополнительные риски для безопасности персонала и надежной работы обо-

рудования. Кроме того, при открытии крышки щита (для измерения) туда попадает внешний воздух, изменяется тепловая картина, поэтому можно пропустить начальную стадию повышения температуры.

Решать задачу эксперт Eaton рекомендует с помощью системы мониторинга температуры Eaton Diagnose System. Система использует беспроводные самозапитывающиеся датчики, которые можно установить там, куда трудно получить доступ при работающей электроустановке. Информация с датчиков собирается коллектором, а оттуда может направляться в используемую ЦОДом систему SCADA или DCIM. Данные о температуре медных проводников и внутри низковольтных комплектных устройств собираются в режиме реального времени, что позволяет зафиксировать начальный этап повышения температуры.

Сегодня заказчики предъявляют все более профессиональные и жесткие требования к характеристикам инженерной инфраструктуры ЦОДов. При этом повышение требований к качеству и надежности зачастую сочетается с необходимостью сокращения сроков реализации проекта. Современные технологии и решения, в первую очередь модульные системы PFM, позволяют удовлетворить этим в чем-то противоречащим друг другу требованиям, т.е. строить ЦОДы быстро и качественно. ИКС

Edge как искусство

Даже те, кто не имеет стратегии в части edge computing, все равно не могут сегодня обойтись без узлов периферийных вычислений. Размер, отказоустойчивость и наполнение таких узлов мы обсуждаем с Владимиром Гречушкиным, руководителем направления по работе со стратегическими заказчиками подразделения Secure Power, Schneider Electric.



– Владимир, перевод термина «edge computing» на русский пока не устоялся – «распределенные», «границные», «периферийные»... Какой вариант предпочитаете вы?

– Мы придерживаемся термина «периферийные вычисления» – в противоположность централизованным. Многие годы происходила централизация средств хранения и обработки данных. Считалось, что чем сильнее централизовать вычислительные ресурсы, тем выше будет эффективность их использования. И это действительно так. За счет виртуализации утилизацию серверов можно вывести на уровень 80–90%.

Сейчас активно идут процессы цифровизации, причем оцифровывается не только то, что раньше было аналоговым, но и то, что раньше вообще никак не было связано с «классическим» ИТ. Повсеместно компании устанавливают множество датчиков, которые генерируют все большие объемы данных. При централизованной модели хранения и обработки эти «сырые» данные необходимо передавать в центр. Возникает проблема ограниченной пропускной способности каналов связи. Особенно она актуальна для сильноудаленных регионов, например, на Севере, где проводится нефтедобыча. Там с каналами связи может быть совсем плохо. Но и при наличии хороших каналов передавать по ним «тяжелый» контент, скажем, сканы и видео, не всегда разумно. Эффективнее обработать его там, где он создан.

Другая тенденция – развитие систем реального времени. При задержках, измеряемых секундами, централизованные системы работать не будут. Взять, например, отслеживание вибрации турбины. Скорость нарастания колебаний в такой системе может измеряться долями секунды, поэтому важна практически мгновенная реакция на негативный тренд. Иначе возможна техногенная катастрофа с человеческими жертвами.

Еще одна тенденция – рост требований к отказоустойчивости. Если система отслеживает тот же производственный процесс, а экскаваторщик по неосторожности перерубил оптический кабель, по которому данные передаются в центральный ЦОД, то локальные узлы должны перейти в автономный режим. А если вся обработка делегирована в центр, то это будет означать просто остановку работы.

Ну и, конечно, безопасность. Даже сырые данные при передаче в центр может быть необходимо защищать от несанк-

ционированного доступа, например – с помощью шифрования, для чего нужен локальный узел, который будет этим заниматься. А шифрование данных, особенно поточных, – процесс трудоемкий, который требует ресурсов на месте.

Поэтому централизованные решения перестали быть достаточными. Необходимо создавать удаленные вычислительные узлы там, где данные генерируются.

– Чем можно объяснить одновременное проявление двух, казалось бы, разнонаправленных тенденций: с одной стороны, централизации (мега- и гиперЦОДы), с другой – децентрализации (edge)?

– Плюсы централизации сохраняются. Те задачи, которые можно централизованно решать в крупных ЦОДах и в облаках, построенных на базе таких ЦОДов, выгоднее решать там. В них в полной мере работает «экономия за счет масштаба». Периферийные вычисления никогда не заменят централизованные облака, и наоборот. Облака и edge-узлы дополняют друг друга. Они будут сосуществовать и развиваться параллельно.

– А средний уровень будет проседать?

– Возможно, сегмент средних ЦОДов будет расти немного медленнее. Но все равно такие ЦОДы будут строиться. Взять, например, крупного заказчика с территориально распределенной структурой. В Москве – центральное облако. На конечных узлах – небольшие edge-ЦОДы. Но ему необходим еще один уровень – региональные ЦОДы, которые будут служить узлами агрегации данных, передаваемых с периферии в центр. Мы получаем трехуровневую архитектуру: периферийные узлы – опорные региональные ЦОДы – центральный ЦОД (облако).

– Согласно исследованию IDC, 60% компаний не имеют стратегии в части edge computing. Говорит ли это об их неготовности внедрять такие решения?

– Давайте спросим у обычных людей, есть ли у них стратегия домашнего бюджета. На вопрос, сформулированный таким образом, многие ответят отрицательно, но на практике они, конечно, планируют свои доходы и расходы. Так и в случае с периферийными вычислениями – стратегии, возможно, нет, а edge-узлы есть. Я скорее удивлен, что только 60% так ответили, это число могло быть и больше.

Еще заказчики не всегда понимают, что то, чем они занимаются, и есть периферийные вычисления. Открытие банковского офиса или нового магазина сегодня почти всегда

связано с развертыванием вычислительного edge-узла, хотя заказчик может и не использовать этот термин.

– **Edge – это вообще про размер? Это обязательно небольшой комплекс?**

– Здесь все зависит от специфики конкретного проекта. Для кого-то edge-ЦОД – даже не стойка, а шкаф на несколько юнитов. В другом случае такой ЦОД реализуется в виде промышленного защищенного шкафа или обычной ИТ-стойки. Это могут быть и десятки стоек. Каких-то жестких ограничений по емкости нет.

– **А edge-узел может быть больше центрального ЦОДа?**

– Почему бы и нет – если на периферии необходимо обрабатывать больше данных, чем в центре. В центре вообще может быть некий арбитр, который будет заниматься координацией и распределением задач по нижележащим узлам.

– **Эксперты рекомендуют рассматривать edge-узлы как критически важные дата-центры с соответствующими средствами отказоустойчивости. Но ведь в виртуализированной среде можно обеспечить надежную работу ИТ-систем и на базе распределенной сети надежных узлов?**

– Существуют разные способы обеспечения отказоустойчивости. Их выбор определяется технологическими, экономическими и другими причинами. Например, можно делать резервирование на уровне шкафа, устанавливая туда два ИБП, два кондиционера и пр. А можно – на уровне нескольких узлов, подключив датчики и контроллеры сразу к двум шкафам, при этом в отдельных шкафах обойтись без резервирования.

Если говорить об обеспечении отказоустойчивости с помощью средств виртуализации, то необходимо оценить экономическую целесообразность. На уровне двух ЦОДов (резервный – основной) все уже отработано. А когда у вас 200 узлов? И в каждый узел надо купить лицензии на ПО, обеспечивающее миграцию ИТ-нагрузки. Это может быть очень затратно.

– **Для отдельных ЦОДов существуют общепринятые методики оценки их отказоустойчивости. А какие подходы можно использовать для оценки надежности сети распределенных периферийных узлов?**

– Отработанной методологии я не встречал. Но она, очевидно, появится.

В целом обеспечение надежности распределенной edge-архитектуры – сложная задача, требующая творческого подхода. Мы готовы браться за такие задачи. Нами были разработаны и внедрены специализированные решения. Мы накопили огромную экспертизу: уже реализованы проекты по построению инфраструктуры периферийных вычислений в ритейле, банковском секторе, промышленности, электроэнергетике и других областях.

– **На удаленных объектах, где разворачиваются edge-ЦОДы, очевиден дефицит квалифицированных специалистов. Как вы предлагаете решать эту проблему?**

– Мониторинг. Устанавливаемое оборудование должно поддерживать централизованный мониторинг. Важно, чтобы удаленный узел мог выдавать максимум информации: о температуре, протечках, статусе ИБП и батареи, состоянии питания до каждой розетки, автоматов на РЩ и т.д.

Представьте себе edge-узел за Полярным кругом. До ближайшего крупного города, где есть специалист, два дня пути. Возникли проблемы в работе такого узла. А что там произошло? Скорее всего, подробной информации нет. Специалист едет туда, выясняет причину, возвращается за запчастями и едет обратно. Время до начала ремонта увеличивается в три раза. При наличии точной диагностической информации проблема решается за один визит специалиста, а возможно, и он не потребуется (например, достаточно дать указание местному электрику заменить автомат).

Все чаще используются средства предиктивной аналитики. У многих заказчиков сотни edge-узлов. На основе данных, собранных с большого числа узлов, можно точнее предсказать негативное развитие ситуации, заранее предотвратив нежелательные последствия. Например, наши системы могут заранее предоставлять рекомендации по замене батарей ИБП. Это важно и для планирования расходов, и для поддержания высокого уровня надежности.

– **Существует ли специфика инженерных систем для edge-узлов?**

– Если говорить о системах электропитания, то заказчики часто выбирают ИБП, которые вместе с автоматами монтируются на DIN-рейку – это очень удобно. Все чаще применяются литий-ионные аккумуляторы. У них много преимуществ, в первую очередь более широкий температурный диапазон и больший срок эксплуатации. Когда расходы, в том числе транспортные, при замене батарей ИБП могут оказаться выше стоимости самого аккумулятора, выгода литий-ионных устройств очевидна.

В части охлаждения используется весь набор решений. Мы не говорим о том, что в каждый edge-узел нужно установить кондиционер. Важно обеспечить необходимые уровни температуры и влажности. Скажем, если потребление ниже 500 Вт на шкаф, то для отвода тепла может быть достаточно вентиляторов. В шкафах с потреблением более 3 кВт уже может потребоваться активное охлаждение.

Для удаленных узлов важна система безопасности. Мы рекомендуем оборудовать их современной СКУД, с помощью которой всегда можно определить, кто из сотрудников имел доступ к оборудованию внутри ИТ-шкафа.

– **А что с ИТ-наполнением? Edge – это все-таки вычислительный узел.**

– У Schneider Electric сформированы технологические альянсы с ведущими производителями ИТ-систем, к примеру Cisco, HPE, Dell, что позволяет нам поставлять комплексные решения. Централизованно, например в Москве, мы или наш партнер можем установить в конструктивы необходимое ИТ-оборудование – серверы, СХД, коммутаторы – и уже готовые edge-узлы направить заказчику. При этом сохраняется гарантия на ИТ-оборудование. На объекте заказчику достаточно установить такой узел (или повесить его на стену), подключить, и все начинает работать. Минимум временных затрат и требований к квалификации персонала.

Системы хранения данных: актуальные тренды



Сергей Орлов,
независимый
эксперт

В последние несколько лет технологии хранения данных развиваются стремительно, растут емкость и производительность, расширяется функциональность СХД. Сегодня для бизнеса важно создать гибкую ИТ-инфраструктуру, готовую к будущим технологиям.

Рынок систем хранения следующего поколения, по данным Mordor Intelligence, достиг в 2018 г. отметки \$21,55 млрд и вырастет к 2024 г. до \$40,8 млрд. Среднегодовой рост составит 11,4%.

Крупнейшим в мире вендором внешних СХД, согласно IDC, остается Dell EMC с долей 30%. Она опережает HPE (11,7%) и NetApp (10,8%), за которыми следуют IBM и Hitachi. Интересно, что другие аналитические агентства дают практически такие же оценки (рис. 1).

К драйверам роста аналитики относят ускоряющееся развитие в области облачных вычислений, больших данных, мобильных услуг и приложений для социальных сетей.

В России основными драйверами роста данного сегмента аналитики IDC традиционно считают госсектор, телеком и компании, реализующие программы цифровой трансформации.

В последнее время произошли заметные изменения в том, как компании получают и хранят свои данные. Перечислим основные тенденции, которые в ближайшей перспективе будут оказывать влияние на рынок корпоративных СХД.

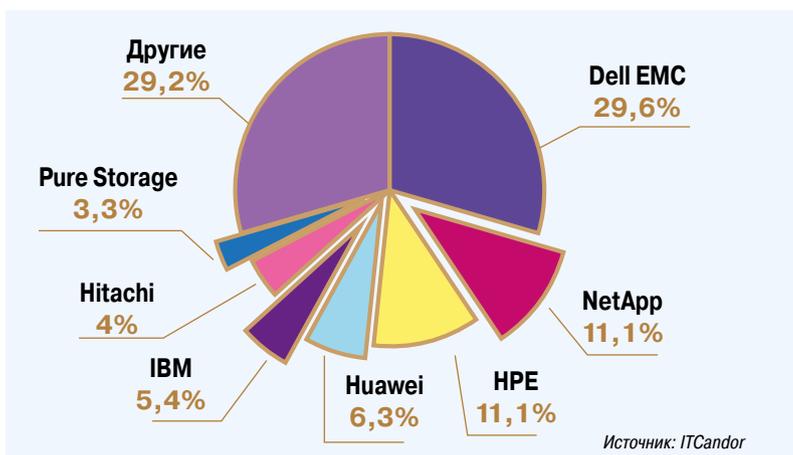
Мультиоблачные хранилища

Такие системы призваны обеспечить мобильность, переносимость данных между несколькими облачными платформами – частными и публичными. Мультиоблачность влияет не только на процессы перемещения, миграции данных, но и на процедуры и организацию доступа приложений к данным.

Многие компании сегодня в сочетании со своей локальной инфраструктурой используют несколько публичных облачных сервисов. Некоторые СХД могут функционировать как компоненты облачной среды, их можно задействовать с публичным облаком и обмениваться с ним данными. Кроме того, отдельные СХД доступны по сервисной модели.

Облачные хранилища приобретают все большую популярность, поскольку позволяют повысить рентабельность инвестиций за счет сниже-

Рис. 1. Доли вендоров на мировом рынке внешних СХД в I квартале 2019 г. ▼



ния затрат на инфраструктуру. Сервисы облачного хранения Cloud Storage расширяют центры обработки данных клиентов до облака, предоставляя хранилище (напрямую подключенное к ресурсам публичного облака) как сервис.

Флеш-накопители

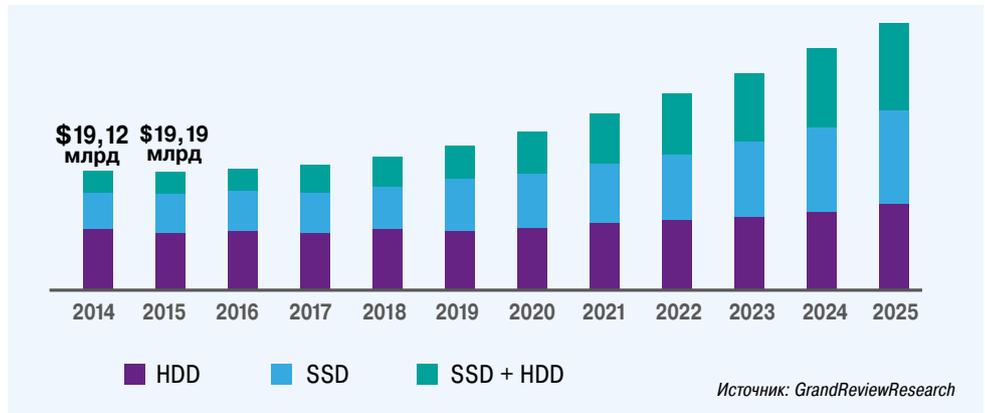
Технологии твердотельных накопителей (SSD) быстро совершенствуются, и в ближайшие годы на рынке появятся новые революционные продукты. Тем временем организации будут продолжать заменять традиционные диски твердотельными накопителями для повышения производительности, простоты управления и энергосбережения. В частности, на крупнейшем в мире североамериканском рынке аналитики ожидают в ближайшие годы двукратного роста спроса на SSD и трехкратного – на гибридные системы (рис. 2). Новые поколения флеш-массивов (Solid State Array, SSA) будут отличать более совершенные средства автоматизации хранения, интеграции с публичными облаками и защиты данных.

Одна из тенденций – увеличение плотности флеш-памяти при снижении стоимости накопителей NAND. По прогнозу Forward Insights, в течение года SSD могут подешеветь в среднем на 30% и более. Либо производители станут продавать SSD большей емкости по той же цене. Однако оценки аналитиков варьируются. Trendfocus прогнозирует, что цена 1 Гбайт NAND упадет до 11,2 центов в 2020-м, до 8,8 в 2021-м и до 7 центов в 2022 г., сокращая разрыв с HDD.

Переход на более плотную технологию 3D NAND также помогает снизить стоимость флеш-памяти. Производители перешли с 32-слойной на 64-слойную 3D-память в 2018 г. и постепенно будут переходить на 96-слойную. Это означает более высокую емкость хранения в том же формфакторе.

Еще одной тенденцией станут чипы NAND с четырьмя уровнями ячеек (QLC), которые могут хранить четыре бита данных на ячейку памяти. Однако в ближайший год в большинстве корпоративных твердотельных накопителей SSD будет применяться трехуровневая флеш-память (TLC) 3D NAND. Доля QLC не превысит 5%.

Между тем, по прогнозам Gartner, к 2021 г. около 20% накопителей на флеш-памяти NAND будут использовать технологию QLC, а к 2025 г. их доля может достичь 60%. QLC 3D NAND предлагает более дешевую альтернативу флеш-памяти по сравнению с TLC и может бросить вызов жестким дискам, особенно в задачах с интенсивным чтением.



Источник: GrandReviewResearch

Следует отметить, что несмотря на серьезное снижение стоимости хранения 1 Гбайт на флеш-накопителях, HDD пока лидирует по емкости поставленных систем, и разрыв в течение последних пяти лет сохраняется (рис. 3).

По мнению аналитиков, системы, построенные на флеш-памяти, дают ценные преимущества компаниям любого масштаба. Переход на массивы с флеш-памятью влечет за собой резкий прирост производительности приложений.

На мировом рынке флеш-массивов лидируют Dell EMC, NetApp и Pure Storage (рис. 4). В России ситуация несколько иная. В первую тройку, по данным IDC, входят Huawei, Dell EMC и HPE – их общая доля приближается к 60%. Причем доля СХД на базе флеш-памяти уже превысила 37% в денежном выражении – заказчики, прежде всего финансовый и телекоммуникационный секторы, продолжают инвестировать в эти высокопроизводительные системы.

NVMe и NVMe-oF

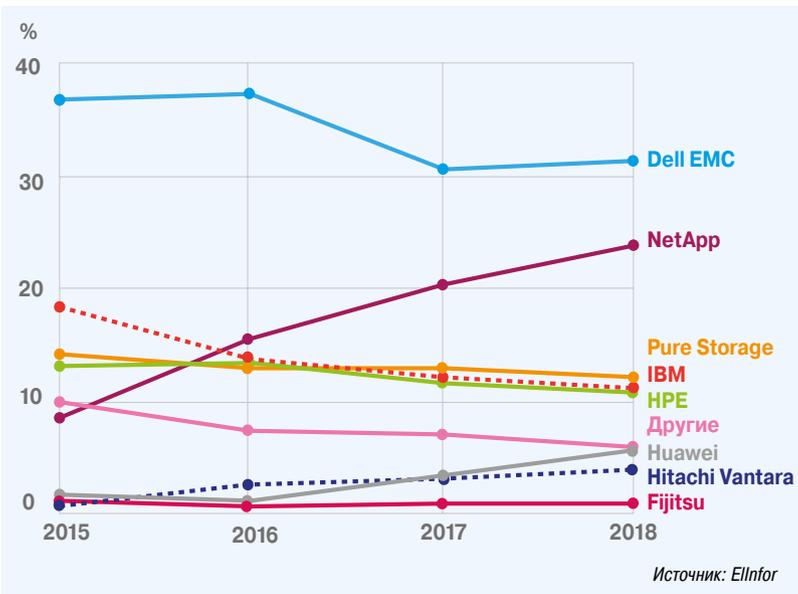
Как считают аналитики, накопители SSD PCIe, которые используют NVMe (Non-Volatile Memory Express), спецификацию протоколов доступа к твердотельным накопителям, подключенным по шине PCI Express, – одна из основных тенденций развития технологий хранения данных.

▲ Рис. 2. Прогноз изменения объемов продаж СХД с накопителями разных типов на североамериканском рынке

Рис. 3. Изменение спроса на разные технологии хранения (по емкости поставленных систем) ▼



Источник: ITCandor



▲ Рис. 4.
Изменение долей
рынка флеш-
массивов
ведущих
вендоров
в 2015–2018 гг.

Протокол NVMe разработан с учетом требований флеш-памяти, он оптимизирован для эффективной работы с SSD. СХД с накопителями NVMe демонстрируют свои лучшие качества при работе с приложениями, чувствительными к задержкам, например с базами данных. NVMe поддерживает до 65536 (64 К) очередей, каждая с глубиной до 65536 команд. Это увеличивает параллелизм при обработке (и как следствие – производительность) и позволяет задействовать преимущества многоядерных процессоров благодаря прямому доступу каждого ядра к SSD. А спецификация NVMe over Fabrics открывает путь к созданию распределенных СХД с низкоталентной фабрикой.

Флеш-массивы с фабрикой NVMe получают распространение быстрее, чем прогнозировали эксперты, но их широкое внедрение в дата-центрах ожидается лишь через несколько лет.

По прогнозу Gartner, к 2021 г. флеш-массивы, использующие NVMe-oF для подключения к серверам и SAN, будут приносить около 30% дохода от поставки СХД. В IDC же считают, что к 2021 г. флеш-массивы с подключениями по NVMe и NVMe-oF обеспечат примерно половину всех доходов от поставок внешних систем хранения.

По мнению аналитиков, NVMe-oF имеет многообещающий потенциал, поскольку обеспечивает чрезвычайно высокую пропускную способность при сверхнизкой задержке. Кроме того, возможность совместного использования систем на флеш-памяти несколькими серверными стойками представляет интерес для организаций с кластерами Oracle Real Application Clusters или другими крупными базами данных.

NVMe-oF расширяет возможности коммутируемого прямого доступа к флеш-памяти, позволяет создавать общие хранилища с такой же стабильной низкой задержкой, как и флеш-память PCIe на обычном сервере.

Кроме того, разрабатываются сетевые транспортные протоколы NVMe для FC-NVMe и различных протоколов удаленного прямого доступа к памяти, включая InfiniBand, RDMA over Converged Ethernet и протокол Internet RDMA.

В настоящее время основные поставщики продуктов NVMe-oF – это Dell EMC, HPE и NetApp.

Использование в СХД памяти SCM

Современная архитектура СХД – это не только поддержка стандарта NVMe. Новая тенденция – использование накопителей класса Storage Class Memory (SCM). Некоторые вендоры уже устанавливают в контроллерах своих СХД подключенные по NVMe модули памяти Intel Optane в качестве кэш-памяти на чтение. В роли кэша на запись выступает оперативная память DRAM или NVRAM.

Благодаря накопителям SCM задержки сокращаются на 40–50%. Применение накопителей Optane в качестве своего рода дополнения к ОЗУ, причем энергонезависимого, – интересное новшество. Как показывает практика, ресурсы ЦП обычно используются на 30%, тогда как оперативная память задействуется полностью. В этих условиях установка модулей Optane – способ повышения производительности. Энергонезависимая память Intel Optane DC с производительностью, близкой к скорости работы оперативной памяти, позволяет ускорить обработку больших наборов данных, например, в задачах искусственного интеллекта.

Производители считают такой подход даже более выигрышным, чем применение для этой цели NVMe-накопителей, поскольку SCM-кэш дает кратный прирост производительности при относительно низких затратах.

Автоматизация хранения: искусственный интеллект и машинное обучение

Внедрение флеш-памяти повлияло не только на производительность СХД, но и на процессы администрирования. Выросли потребности в эффективности защиты данных от развивающихся угроз, атак, сбоев системы и человеческих ошибок. В результате организации начинают инвестировать в комплексные подходы и инструменты защиты данных, средства автоматизации операций.

Автоматизация ИТ-инфраструктуры имеет целью повышение эффективности, снижение затрат на администрирование и исключение ошибок. Автоматизация хранения данных, в том числе на основе искусственного интеллекта, станет типовым подходом.

Аналитика с применением ИИ и машинного обучения позволяет прогнозировать использование емкости хранилища, пометать неактивные или



◀ В массиве Dell EMC PowerMax поддержка NVMe в сочетании с памятью SCM позволяет получить систему хранения, которая обеспечивает до 15 млн IOPS, пропускную способность до 350 Гбайт/с и задержку при чтении менее 100 мкс.

Новые массивы хранения HPE Nimble с поддержкой NVMe и SCM предназначены для приложений аналитики, требующих мгновенных результатов. ▶



редко используемые данные для их перемещения на нижние уровни хранения, выявлять потенциальные риски несоблюдения нормативных требований, например, к хранению персональных данных. Как ожидается, сегмент продуктов на основе искусственного интеллекта и машинного обучения, предназначенных для управления большими объемами данных и их анализа, будет быстро расти. По мере увеличения сложности данных и ИТ они станут распространяться все шире.

Например, компания Igneous Systems анонсировала продукты DataDiscover и DataFlow, которые индексируют и классифицируют неструктурированные данные и интеллектуально перемещают их. Поставщики массивов, включая Pure Storage, NetApp и Dell EMC, поддерживают видеокарты NVIDIA для ускорения аналитики с применением глубокого обучения.

Алгоритмы искусственного интеллекта и машинного обучения могут использоваться для автоматизации развертывания СХД. Эти технологии полезны для оптимизации хранилища, особенно когда речь идет о многоуровневом размещении данных.

Например, в массиве Dell EMC PowerMax система задействует встроенные механизмы машинного обучения для автоматического размещения данных на основе профиля ввода-вывода на носителях соответствующего типа. Их цель – получить максимальную производительность при минимальных затратах.

Основная мотивация использования ИИ в корпоративной среде, по данным опроса Gartner, – это потребность в автоматизации повторяющихся задач (на что указывают 66% респондентов), улучшение клиентского опыта (63%), сокращение затрат (47%), упрощенное выполнение комплексных задач (40%), желание увеличить выручку (27%), конкурентное давление в отрасли (26%) и стремление сократить штат (13%). К основным препятствиям использования ИИ аналитики относят нехватку соответствующих навыков у персонала (56%) и непонимание преимуществ ИИ и принципов его использования (42%).

Что выбрать?

Вендоры продолжают совершенствовать линейки СХД и внедрять новейшие технологии для эффективной работы с таким ценным активом, как данные. Новые решения стали ответом на актуальные потребности ИТ-отрасли в работе с облачными технологиями, автоматизации и оптимизации задач управления и обработки данных.

Как же выбрать систему, оптимальную по соотношению функциональность/цена/качество? В зависимости от решаемой задачи СХД настраиваются, работают, да и позиционируются вендорами по-разному. Зачастую решение разрабатывается для конкретной цели. Например, СУБД характеризуется транзакционной, а система видеонаблюдения – потоковой нагрузкой. Поэтому общая тенденция – выбор специализированной системы в расчете на ту или иную задачу.

Нужно сформулировать основные требования к системе хранения, такие как надежность, функциональность, эксплуатационные характеристики, капитальные/эксплуатационные затраты. Если для нагруженных систем предпочтительнее будет задействовать флеш-массив, то для почтовых сервисов или систем резервного копирования вполне подойдет гибридное решение или СХД на традиционных дисках (HDD).

Четкое понимание назначения системы поможет определиться с ее функциональностью. Нередко она избыточна: часть функций не задействована или используется не по назначению, увеличивая при этом конечную стоимость решения.

Некоторые функции, такие как сжатие данных и дедупликация, могут влиять на производительность или пропускную способность. Поэтому следует исходить из минимально необходимой функциональности. Нужно понять, из чего складывается стоимость эксплуатации решения, как лицензируется расширение, во что выливается замена диска или контроллера, каков запас времени на устранение той или иной аварийной ситуации. Все это поможет выбрать нужную СХД и оптимизировать затраты. ИКС

Edge-ЦОД Rittal для промышленности

Компания Rittal предлагает Edge-ЦОДы повышенной защищенности для использования в производственных цехах.

Новая архитектура – новые требования к инфраструктуре

Россия стоит на пороге четвертой промышленной революции – массового внедрения киберфизических систем в производство. Основой для перехода к Индустрии 4.0 выступает промышленный интернет вещей. Датчики устанавливаются повсюду, вплоть до оснащенных микропроцессорным модулем «умных» касок у рабочих, которые передают телеметрические данные об их местонахождении и состоянии здоровья. Оптимизируются и автоматизируются все процессы, от непосредственно производства до логистики и систем охраны труда. Для проектирования и прогнозирования поведения промышленных систем начинают использовать виртуальные прототипы – цифровые двойники, результаты прогнозирования интегрируются в производственные процессы, все стадии которых контролируются с помощью цифровых технологий.

С обработкой резко возросших объемов информации уже не справляются традиционные ИТ-архитектуры, включающие в себя корпоративные дата-центры, каналы передачи данных и облака. Как раз перегрузка каналов передачи данных привела к необходимости создания многоуровневых архитектур с предварительной обработкой и хранением части информации на нижнем уровне, ближе к месту сбора данных. Промышленность переходит к установке небольших ЦОДов в непосредственной близости к технологическим линиям, складам и т.д., где требуются локальная обработка и хранение больших объемов данных с последующей передачей агрегированной информации на более высокий уровень.

Организовать небольшую серверную в специально предназначенном для этого помещении не проблема: достаточно установить шкаф с перфорацией, через которую подается воздух, и оборудовать помещение кондиционером. Проблема – обеспечить надежную работу периферийного ЦОДа в месте, не отвечающем требованиям чистоты для размещения ИТ-инфраструктуры, в неблагоприятных условиях: в цехах заводов с агрессивными средами, повышенной влажностью или запыленностью; в больших ангарах со значительным суточным перепадом температур; на удаленных объектах с повышенной опасностью вандализма и несанкционированного доступа; наконец, даже прямо под открытым небом. То есть не там, где можно, а там, где нужно клиенту.

В решении этой проблемы способна помочь компания Rittal, имеющая богатый опыт создания комплексных решений для размещения активного оборудования в различ-

ных промышленных средах, в том числе на нефтегазовых и химических заводах, на пищевом производстве, в угольной и обрабатывающей промышленности.

Новым ЦОДам – проверенные решения

В Европе тема edge-ЦОДов (EdgeDC) в промышленности стала актуальна еще четыре года назад. Появилась потребность в резервных и дополнительных серверных, потом небольшие дата-центры начали размещать в цехах. При этом возникла проблема обеспечения их бесперебойной работы в неблагоприятных условиях, ведь надежность системы определяется надежностью всех ее узлов. Бизнес предъявляет к Edge-ЦОДам Rittal такие же требования по отказоустойчивости, как и к большим дата-центрам. Пользователя не интересует, где произошел отказ в работе, его волнует непрерывность производства.

У Rittal уже был набор решений для промышленности, имелся и большой опыт создания систем для ИТ. Компания смогла оперативно ответить на запрос рынка и организовать выпуск надежной инфраструктуры ЦОДа в компактном корпусе, так что при выносе части инфраструктуры на границу сети система в целом не становится менее надежной.

Среди широкого ассортимента решений Rittal – шкафы, оболочки, системы охлаждения ИТ-оборудования в заводских условиях. Компания предлагает устанавливать в промышленных помещениях Edge-ЦОДы Rittal в виде закрытых шкафов с классом защиты IP55 или даже IP66, которые предохраняют активное оборудование от влаги и разных видов пыли. Есть также опция обеспечения электромагнитной совместимости для корпуса Edge-ЦОДа. Шкафы могут выпускаться в корпусах из нержавеющей стали, со специальными покрытиями для химической промышленности, которые защищают оборудование даже в случае солевого тумана. Специальные виды нержавеющей стали обеспечивают использование Edge-ЦОДов Rittal в цехах заводов пищевой промышленности. Применяются локальные системы охлаждения, зависящие от внешних условий, например холодильные агрегаты, размещаемые снаружи шкафа.

В промышленности востребованы решения без вывода фреоновых трасс наружу – двухконтурная система охлаждения работает с выбросом тепла прямо в помещение, при этом внешний воздух двигается по изолированному



Александр Кюн,
ведущий менеджер
по продукции для
ИТ-инфраструктуры, Rittal

внешнему контуру и не попадает внутрь. Компания предлагает Edge-ЦОД с такой нетрадиционной для ИТ системой охлаждения. Установить решение просто – доставляется собранный Edge-ЦОД Rittal в виде шкафа, включается питание, и система работает. В большом цеху тепло легко рассеивается, а внутри шкафа сохраняется идеальная температура 20°C.

Неспециализированное оборудование, такое как ИБП, системы мониторинга и пожаротушения, размещается внутри шкафа. Используется обычное непромышленное оборудование – отличия промышленных Edge-ЦОДов Rittal от обычных кроются в реализации оболочек и систем жизнеобеспечения.

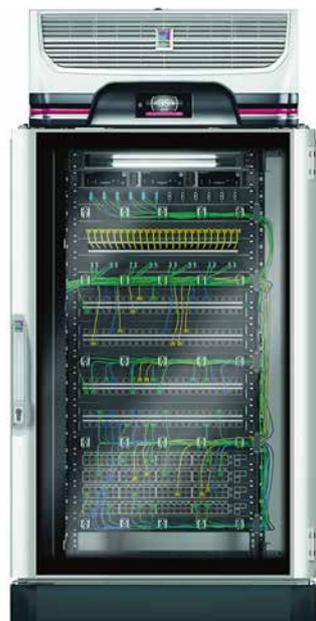
Преимущества промышленных решений Rittal

Предлагаемые компанией решения обладают рядом преимуществ. Первое – это надежность, обеспечиваемая большим опытом работы и безупречной репутацией компании Rittal.

Решения не требуют отдельного помещения и специальных защитных оболочек, их можно устанавливать в любом месте, даже на улице. Например, edge-ЦОДы могут использоваться в системах охраны периметра предприятия для предварительного анализа информации систем видеонаблюдения. В уличных шкафах размещаются видеосерверы, ИБП и прочая инфраструктура охранных систем. Не нужно строить дополнительное помещение или ставить контейнер – достаточно отдельного шкафа с двойными стенками и специальной уличной крышей, в котором путем охлаждения в летний сезон и обогрева в зимний обеспечивается требуемая температура. В портфеле компании есть Edge-ЦОДы, работающие при внешних температурах до -40°C. На российском рынке востребованы решения с высокой степенью защиты от вандализма. В этом случае поможет антивандальный сейф Rittal.

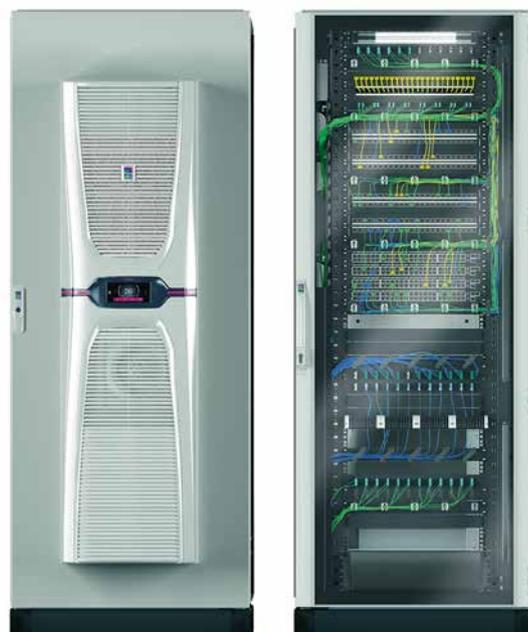
У решений Rittal есть и другие преимущества – компания предлагает для промышленности базовое решение из коробки, которое не надо дорабатывать, доукомплектовывать, увеличивая занимаемый объем и вес. Компания обладает большим портфелем стандартизированных edge-решений для производства, которые собираются специалистами Rittal на месте. Это prefab-ЦОДы. Заказчикам не надо думать об их проектировании – они получают устройства с заранее заданными параметрами охлаждения и безопасности.

Нагрузочная способность шкафа Rittal достигает 1,5 т. В промышленности периферийные ЦОДы чаще всего разме-



◀ Компактный Edge-ЦОД Rittal

Модульный Edge-ЦОД Rittal ▶



щают на первых этажах цехов на бетонных полах, которые с большим запасом выдерживают такой вес. Но у компании есть и портфель решений, сформированный с учетом нагрузочной способности перекрытий до 700 кг/кв. м и позволяющий при необходимости размещать периферийные дата-центры на других этажах. Компактные решения Rittal вписываются в нагрузку около 400 кг/кв. м, что особенно важно для старых производственных зданий со сниженной несущей способностью перекрытий.

Чаще всего в промышленности используют edge-ЦОДы, размещенные в одном шкафу. Но у компании есть и масштабируемые модульные решения из нескольких шкафов, соединенных в линейку. Например, Edge-ЦОД Rittal из трех-пяти шкафов, в которых часть места занимает инженерное оборудование, а остальное место предназначено для оборудования клиента. Такие Edge-ЦОДы можно масштабировать добавлением как дополнительных шкафов, так и целых модулей. При этом в каждом конкретном случае можно оптимизировать набор оборудования под конкретные требования по нагрузочной способности пола, антивандальным свойствам, повышенной тепловой нагрузке от активного оборудования и многим другим.

Логистическая сеть Rittal в России включает четыре больших склада – в Москве, Санкт-Петербурге, Екатеринбурге и Новосибирске. Это позволяет ускорить и упростить доставку в любую точку России.

Компания Rittal готова взять на себя инженерную часть построения ИТ-обеспечения бизнеса, предоставляя ИТ-специалистам клиента возможность сосредоточиться непосредственно на серверах, СХД и другом активном оборудовании.



**ООО «Риттал», 125252, Москва,
ул. Авиаконструктора Микояна, 12,
БЦ "Линкор", 4 этаж
тел. (495) 775-0230, факс (495) 775-0239
info@rittal.ru, www.rittal.ru**

Будущее сейчас: технологии ИИ в дата-центрах



Ирина Рундель,
аналитик,
Colobridge

Гетерогенность современных ИТ-систем и тенденция к автоматизации и оркестровке ИТ-операций диктуют новые правила администрирования ИТ-инфраструктуры ЦОДов.

Чтобы эффективно использовать вычислительные мощности дата-центров, специалисты должны иметь целостное представление о работе всех его компонентов в режиме реального времени. В этом им приходят на помощь решения на основе технологий искусственного интеллекта.

Новые требования = новые технологии

Из-за непрерывной генерации новых данных, которым нужно гарантировать надежное хранение и быстрый доступ к ним, требования к ЦОДам в последнее время заметно возросли. В первую очередь дата-центры стараются снизить энергопотребление (и, соответственно, операционные расходы), одновременно повышая производительность и доступность инфраструктуры. Задача не из легких, и пока ее пробуют решить с помощью ПО на основе машинного обучения и анализа больших данных. Аналитики Gartner считают, что к 2020 г. более 30% ЦОДов, которые не смогут внедрить эти технологии, будут обречены на потерю работоспособности и рентабельности.

Отметим, что машинное обучение и некоторые виды когнитивных вычислений уже сейчас применяются в дата-центрах, например для того, чтобы обеспечить самовосстановление сервисов, рационально использовать аппаратные средства и снизить расходы на эксплуатацию, а также для умного управления физической площадкой и интеллектуальной автоматизации процессов. Эти технологии позволяют операторам ЦОДов увеличивать рабочую нагрузку на один процессор за счет анализа большого объема разрозненных данных, получаемых в режиме реального времени.

Какие решения существуют сейчас?

Современный ЦОД можно сравнить с оркестром, в котором множество механических и электрических компонентов должны действовать синхронно и слаженно, «прислушиваясь» друг к другу. Однако отследить огромное количество взаимных зависимостей, которые присутствуют в дата-центрах, чтобы в итоге оптимизировать и автоматизировать все ИТ-операции, человеку, увы, не под силу. Зато неплохие резуль-

таты показывают решения, в основе которых лежат алгоритмы машинного обучения и методы анализа больших данных. Различные экспертные системы, системы рекомендаций на основе нейронных сетей, предиктивное моделирование ЦОДа, интеллектуальные хранилища, когнитивные сети, системы кибербезопасности и т.д. – все это должно изменить привычную работу дата-центров и, возможно, сам их формат уже в недалеком будущем.

Ниже мы представляем краткий обзор продуктов, которые уже успешно применяются в современных дата-центрах, и некоторых моделей, которые только обсуждаются в исследовательских кругах. Все они направлены на то, чтобы облегчить повседневную работу ИТ-администратора ЦОДа и поддержать его в принятии правильных решений.

Экспертная система Cognitive Insights от Logz.io

Эту ИИ-платформу с технологией Unified Machine Intelligence (UMI) разработали израильские программисты. Она осуществляет интеллектуальный анализ логов, на основе которых потом строит прогнозы и предсказывает возможные перебои в работе сервисов дата-центра.

В основе UMI лежат алгоритмы машинного обучения с учителем, которые сопоставляют данные о взаимодействии человека с журналом логов и релевантную информацию, опубликованную на известных форумах (StackOverflow или Serverfault) и репозиториях с открытым исходным кодом (GitHub), пытаясь найти взаимосвязь между ними. Затем система отображает полученные результаты в пользовательском интерфейсе Logz.io. Поскольку количество логов огромно, а большая их часть малоинформативна, применение Cognitive Insights значительно сокращает время поиска верного решения в случае критических инцидентов, которые ставят под угрозу стабильность ИТ-системы.

Когнитивное DCIM-решение от Nlyte и IBM

Компания Nlyte, которая занимается разработкой ПО для управления инфраструктурой дата-центров (DCIM) с 2004 г., имеет в своей линейке продукт Nlyte Energy Optimizer (NEO). В режиме реального времени он осуществляет мониторинг энергопотребления и тенденций его изменения, а также тревожных событий в информационной и телекоммуникационной инфраструктуре ЦОДа.

NEO работает в тесной связке с решением IBM под названием PМО (Predictive Maintenance and Optimization). К данным, собранным с помощью NEO, PМО применяет заранее определенные ша-

блоны, выявленные с помощью алгоритмов машинного обучения на основе данных из всех распределенных и виртуальных источников (IBM Watson). Полученные результаты NEO используют для подготовки отчетов о работе конкретного дата-центра или принятия нужных мер (например, контроля заданных точек на выделяющем тепло оборудовании). Тандем NEO и PМО позволяет собрать данные из всех распределенных источников, таких как серверы, системы отопления, вентиляции и кондиционирования, распределители питания, построить обширную аналитику и визуализировать результаты, что опять же помогает ИТ-администраторам быстро определить текущее положение дел в дата-центре.

Предиктивное моделирование дата-центров: решения SAP и Future Facilities

Моделирование дата-центров становится все популярнее. Наиболее известные на сегодня вендоры – SAP с решением IT Operations Analytics (ITOA) и Future Facilities с 6SigmaDCX. Их продукты расчитаны главным образом на провайдеров услуг colocation и ЦОДы малых и средних компаний.

В SAP рассказывают, что идея ПО для интеллектуального анализа и моделирования дата-центра возникла из собственного опыта компании. По данным ресурса datacenter-insider.de, в своих ЦОДах SAP регистрировала полмиллиарда событий каждый день и использовала до 20 (!) программ мониторинга ИТ-операций. Ее решение ITOA позволило объединить функциональность этого множества систем в одном пакете.

В свою очередь, решение 6SigmaDCX от Future Facilities интегрируется с инструментами DCIM от ведущих поставщиков и собирает данные о состоянии серверов, энергопотреблении, температуре в помещении, режимах кондиционирования и т.д. в качестве отправной точки для моделирования будущих событий в ЦОДе. Это дает провайдерам услуг colocation возможность анализировать отчеты об изменениях температуры, работе систем вентиляции и т.п., а также моделировать размещение различных компонентов, не оказывая влияния на повседневную работу ЦОДа. ПО также имеет доступ к библиотеке, включающей параметры более 800 ACU (Array Configuration Utility) и 2400 серверов, и использует технические данные этих устройств для моделирования виртуального дата-центра.

Интеллектуальное хранилище Nimble Storage от HPE

Сегодня дисковые системы хранения данных нередко заменяются all-flash-массивами, так как они обеспечивают лучшую производительность. Но хранилище – лишь часть ИТ-инфраструктуры,

которая должна слаженно работать с другими компонентами и, что не менее важно, учитывать особенности различных приложений.



Все массивы памяти Nimble с самого начала оснащаются датчиками с предустановленным специализированным ПО, с помощью которого информация об устройствах отправляется в облачную систему поддержки HPE InfoSight. В систему передаются данные о пропускной способности, параметры ввода-вывода (IOPS), время задержки, а также данные мониторинга работы приложений, пиковые нагрузки и т.д. Решение InfoSight создано в результате анализа базы знаний, собранных со всех машин, использующих Nimble Storage. На сегодня в мире работает 30 тыс. хранилищ Nimble, с которых каждые пять минут в облако InfoSight отправляются данные о конфигурации, состоянии процессоров, DRAM, сетевых компонентов, производительности приложений и т.п. InfoSight сравнивает между собой информацию, полученную от разных машин, ищет нерегулярности или события, являющиеся предвестниками возникновения ошибок, а потом отправляет сообщения или прогнозы клиентам. Причем, по данным HPE, с помощью решения InfoSight можно автоматически устранять 86% зарегистрированных ошибок, из которых 54% связаны не с хранилищами данных, а с другими компонентами ЦОДа.

Системы рекомендаций на основе искусственных нейронных сетей

Пару лет назад ИТ-ресурсы пестрили сообщениями о том, как Google сумела сократить энергопотребление в своих ЦОДах на 40% с помощью технологии DeepMind. Система DeepMind AI анализировала значения 120 переменных, которые отражают состояние таких компонентов ЦОДа, как вентиляторы и система охлаждения, общую загрузку серверов (в киловаттах) и др. По данным Telehouse, в 2014 г. Google потребила 4 402 836 МВт•ч электроэнергии, поэтому можно предположить, что DeepMind помогла компании сэкономить миллионы долларов.

Искусственные нейронные сети оказались мощным инструментом для интеллектуального анализа, в частности для вычисления корреля-

ции между огромным количеством переменных. Например, сеть может предложить регулировку температуры охлаждающей воды в определенной области дата-центра или указать наиболее подходящее время для переноса рабочих нагрузок в случае обновления оборудования.

Когнитивные сети, определяемые знаниями

Одна из наиболее сложных и критически важных задач для любого ЦОДа – оптимизация производительности сети. Как показало недавнее исследование IDG, сегодня большой популярностью пользуется технология SDN (Software-Defined Network), в которой централизованная функция управления позволяет обозревать все процессы, происходящие в сети. В свое время ее появление действительно оказалось прорывом, и сейчас некоторые эксперты склоняются к тому, что следующим этапом эволюции сетей станет Knowledge-Defined Network – сеть, определяемая знаниями, действующая на основе алгоритмов машинного обучения. Маршрутизация, распределение ресурсов, виртуализация сетевых функций (NFV), цепочка сервисных функций (Service Function Chaining, SFC), обнаружение аномалий, анализ загруженности сети – все эти пункты способна взять на себя KDN.

Напомним, сеть SDN имеет три уровня – уровень данных (отвечает за хранение, передачу и обработку пакетов данных), уровень контроля (обменивается информацией о рабочем состоянии сети с уровнем данных для того, чтобы обновить на нем правила сопоставления и обработки пакетов) и уровень управления (обеспечивает правильную работу и производительность сети в долгосрочной перспективе, определяет топологию сети, конфигурирование и настройку сетевых устройств). В отличие от SDN, сеть, определяемая знаниями, предполагает наличие четвертого уровня – уровня знаний (Knowledge Plane, KP), который обеспечивает возможность интегрировать поведенческие модели сети и процессы, направленные на автоматическое принятие решений, в сеть SDN.

По сути, в рамках KP с помощью алгоритмов машинного обучения осуществляется анализ сетевых данных, а полученные результаты используются для принятия решений (как автоматически, так с вмешательством человека).

В рамках KDN подлежат анализу такие категории данных:

- данные уровня пакета и потока, анализируемые обычно системами DPI (Deep Packet Inspection) – гранулярность потока данных и соответствующие характеристики трафика;
- состояние сети – физические, топологические и логические конфигурации сети;

- состояние контроля и управления – информация, содержащаяся в контроллере SDN и инфраструктуре управления: политика сети, виртуальная топология, информация, касающаяся приложений, и т.д.;
- телеметрия на уровне обслуживания – данные о поведении приложения или сервиса в связке с производительностью сети, ее загрузкой и настройкой;
- внешняя информация.

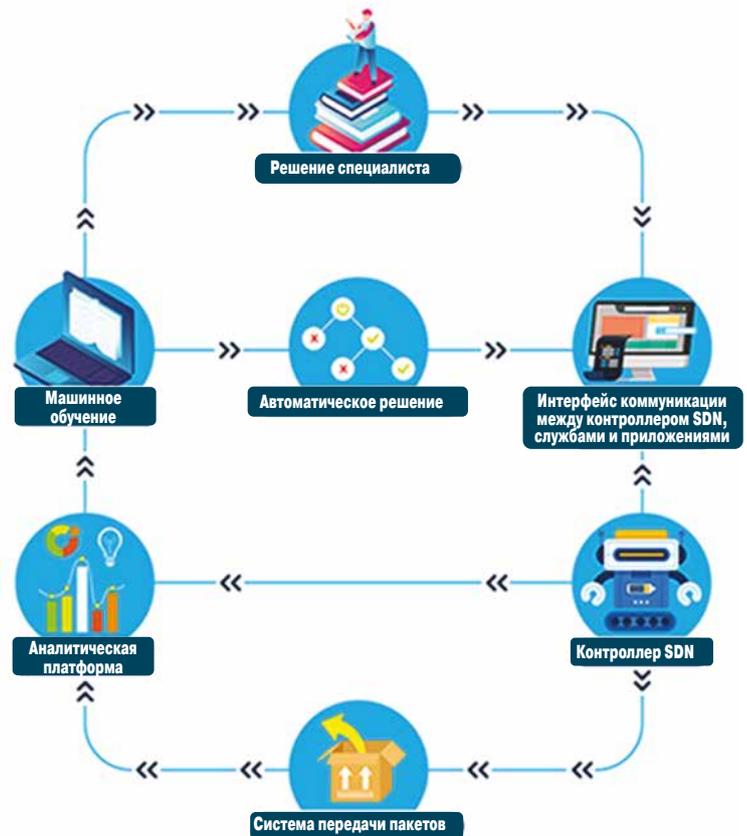
Сетевая модель, полученная с помощью алгоритмов машинного обучения – с учителем или с подкреплением, может использоваться для автоматизации работы и оптимизации текущей конфигурации сети. При обучении без учителя сделанные моделью выводы можно применить для автоматического улучшения производительности сети через интерфейс контроллера SDN. Например, определив корреляцию между трафиком, маршрутизацией, топологией и результирующей задержкой, можно смоделировать оптимальные конфигурации маршрутизации, которые минимизируют задержку. Модель, полученную путем обучения с учителем, можно использовать для тестирования предварительных изменений в системе или в качестве инструмента оценки производительности и анализа «что-если».

Однако отметим, что KDN – пока лишь концепция, живущая в умах ученых. Одна из серьезных трудностей при применении машинного обучения для интеллектуального управления сетью заключается в том, что сети представляют собой распределенные системы, где каждый узел (коммутатор, маршрутизатор) имеет только «частичное представление» о работе системы в целом, поэтому возникает проблема репрезентативности данных, на основе которых будет строиться обучаемая модель.

Когнитивная кибербезопасность

Ученые ожидают, что когнитивные сети не только помогут оптимизировать производительность сети, но и выведут кибербезопасность на новый уровень. Например, британская компания Darktrace использует машинное обучение для мониторинга нормального поведения сети, что позволяет вовремя обнаружить и устранить угрозы, вызванные отклонением от этой нормы. Пока дата-центры пытаются предотвратить киберриски путем ограничения доступа к сетям и создания «непроницаемых» межсетевых экранов. Однако из-за постоянного увеличения потока пользователей такие методы скоро не смогут гарантировать должный уровень безопасности.

Эксперты пророчат, что именно когнитивная киберзащита в конечном счете заменит обычные си-



▲ Схема использования сети KDN

стемы обнаружения инцидентов информационной безопасности. Но и здесь разработчики сталкиваются с проблемами: например, злоумышленники могут обучать когнитивные системы на фальшивых данных с помощью ботнетов.

■ ■ ■

Сегодня технологии искусственного интеллекта влияют на развитие ЦОДов минимум двумя способами. Во-первых, приложениям на основе ИИ самим нужно больше вычислительных мощностей, которые им должен обеспечить дата-центр. В связи с этим все чаще обсуждаются различные варианты так называемых ускорителей ИИ. Во-вторых, приложения, использующие алгоритмы машинного обучения, способны повысить производительность ЦОДа и уже это делают. В частности, решения для управления инфраструктурой дата-центров, в основе которых лежат технологии ИИ, пользуются большим спросом. Они помогают обрабатывать данные, получаемые от различных компонентов ЦОДа, в режиме реального времени, строить прогнозы и давать рекомендации специалистам. Конечно, говорить о том, что это ПО способно заменить человека, пока не приходится. Но одно можно сказать точно: взяв на себя рутинную работу, эти приложения помогают ИТ-администраторам сосредоточиться на более важных и творческих аспектах поддержания эффективности ЦОДа, а в форс-мажорных ситуациях принять самое верное решение. ИКС

Нейронные сети в глубоком обучении

Андрей Пивоваров, руководитель группы перспективных технологий предпроектного консалтинга, Oracle в России и СНГ

Нейронные сети – алгоритмы, имитирующие работу мозга, – в современном быстро развивающемся мире машинного обучения вызывают большой интерес, поскольку могут научиться распознавать шаблоны.

Известный пример – нейронная сеть, которая способна научиться распознавать, есть на картинке кошка или нет. В этой статье мы опишем различные типы нейронных сетей, расскажем, как они работают и где используются.

Как устроены нейронные сети

Рассмотрим сначала базовые компоненты нейронной сети. Это не сложно, нужно прояснить лишь пять понятий (рис. 1):

- нейроны;
- входы;
- выходы (функции активации);
- веса;
- смещения.

Нейроны принимают решения. У каждого нейрона есть один или несколько входов и один выход, называемый также функцией активации. Выход одного нейрона может служить входом для другого нейрона (или нескольких нейронов) или быть выходом для сети в целом. Некоторые входные данные более важны, чем другие, и поэтому имеют соответствующий вес. Нейроны сами «активируют» или изменяют свои выходы в зависимости от входных весов. Как быстро они срабатывают, зависит от их смещения.

На рис. 1 не показаны вес и смещение – обычно это числа с плавающей запятой в диапазоне от 0 до 1. Простейший пример выхода (функции активации) нейрона – переключатель вкл./выкл., но эта функция может принимать различные формы. В некоторых случаях значение на выходе может быть меньше нуля.

Рис. 1. Компоненты нейронной сети ▼



Примеры работы нейронных сетей

Теперь, когда есть базовые компоненты, соберем из них простую нейронную сеть. На рис. 2 показана нейронная сеть, которая используется для распознавания рукописных цифр.

Слева – входы, на которые подаются отсканированные изображения рукописных цифр размером 28 x 28 пикселей. На рис. 2 показаны только восемь входов, но в действительности их 784 – по одному на каждый из 784 пикселей в изображении. Справа – выходы. Чтобы результат был однозначным, при обработке каждого нового изображения должен срабатывать один и только один из нейронов. В середине – скрытый слой. Он назван так потому, что недоступен непосредственно. Такую нейронную сеть можно обучить распознавать отсканированные изображения рукописных цифр с высокой точностью.

Но подобная нейронная сеть – еще не сеть глубокого обучения. Она слишком проста: скрытый слой только один. Точка отсчета – как минимум два скрытых слоя (рис. 3).

Зачем нужны скрытые слои? Каждому из нейронов во входном слое соответствует определенный пиксель на картинке, в то время как выходные нейроны выдают результат распознавания всего изображения (например, если срабатывает нейрон 7, то на картинке скорее всего семерка). Скрытые слои соответствуют компонентам изображения. Они могут «распознавать» кривую, диагональ или замкнутый контур. Важно, что компоненты в скрытых слоях соответствуют определенной области исходного изображения. Так и должно быть – они жестко привязаны к конкретным пикселям слева.

Однако сеть такого типа, как на рис. 3, не способна дать ответ даже на вопрос, сколько лошадей на картинке.

У человека не возникнет проблем с подсчетом числа лошадей (конечно, если это не табун). Он легко распознает характерные очертания лошади, независимо от того, где на картинке она находится. И это замечательно, потому что мир, в котором мы живем, требует, чтобы мы умели

распознавать объекты, которые располагаются перед нами или сбоку от нас, даже если они частично скрыты.

Для решения таких задач потребуется нейронная сеть другого типа, подобная показанной на рис. 4: сверточная нейронная сеть.

Представим, что мы снова работаем с изображениями размером 28 x 28 пикселей, но на этот раз мы не можем полагаться на то, что образ только один, и что он находится в центре. Рассмотрим логику первого скрытого слоя. Все нейроны теперь связаны не с одним пикселем, а с конкретными перекрывающимися областями входного изображения (в данном случае это область 5 x 5 пикселей).

Если начать с данной базовой структуры и включать дополнительную обработку, то можно построить нейронную сеть, которая способна идентифицировать элементы независимо от их расположения. Кстати, нейроны в зрительных участках коры головного мозга живых существ, в том числе людей, работают аналогичным образом. Некоторые нейроны реагируют только на изображение в определенных областях поля зрения.

Сверточные нейронные сети – основа алгоритмов распознавания изображений. Но для обработки естественного языка они не слишком пригодны. Определение значения написанного или произнесенного слова весьма отличается от обработки независимых изображений. Язык контекстуален, т.е. отдельные слова должны обрабатываться с учетом соседних слов.

Когда встает задача обработки предложения, нужно учитывать как минимум три момента: первые два – это значение отдельных слов и синтаксис или грамматика предложения (правила порядка слов, структура предложения и т.д.).

Рассмотрим предложение: «Я пеку радужный пирог и хочу добавить в тесто разные...». Какое слово пропущено? Вы можете догадаться, только взглянув на первую часть предложения. В радуге много разных цветов, поэтому в тесто потребуется добавить разные пищевые красители.

Рекуррентные нейронные сети

Чтобы сеть могла прийти к такому ответу, в качестве входных данных для нахождения следующего слова необходимо использовать значения предыдущих слов в предложении. Это не что иное, как цикл обратной связи, который нам пока не встречался. Сети с петлями обратной связи (рис. 5) называются рекуррентными нейронными сетями.

Обратите внимание, что выходные данные возвращаются и снова подаются на вход. Если эту схему «развернуть», то получится структура, подобная приведенной на рис. 6.

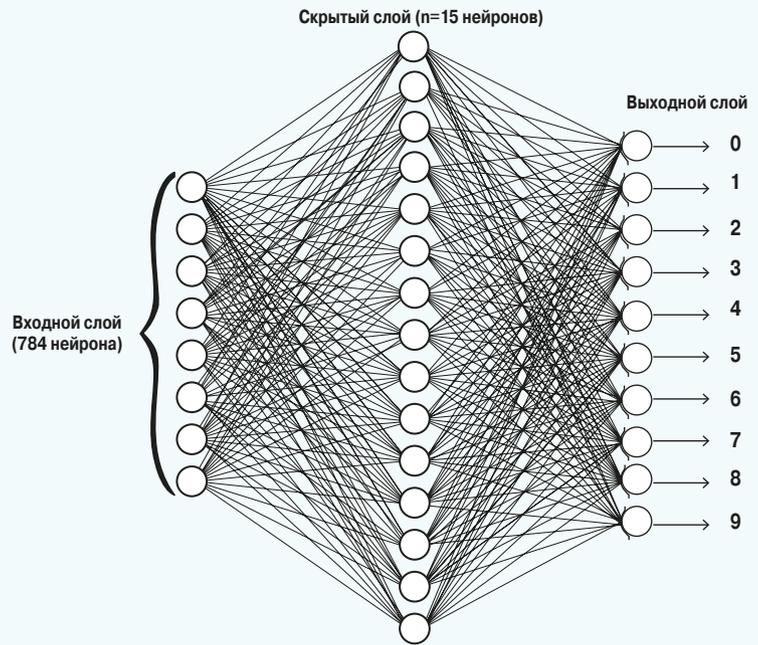


Рис. 2. Пример простейшей нейронной сети ▲

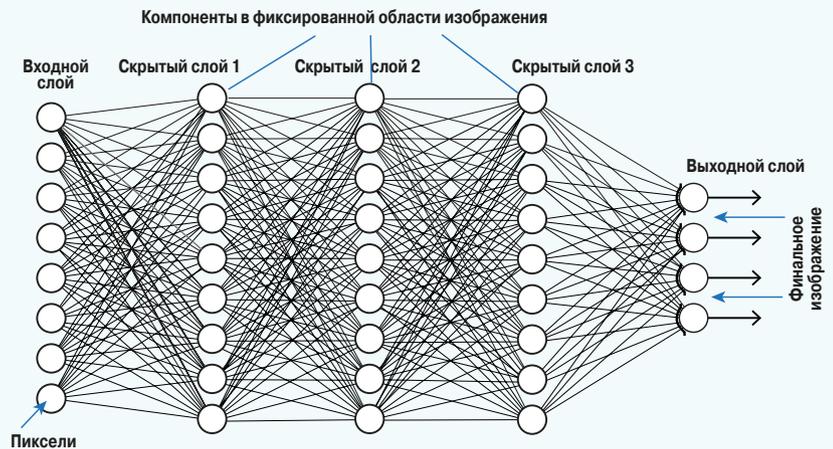


Рис. 3. Нейронная сеть глубокого обучения ▲

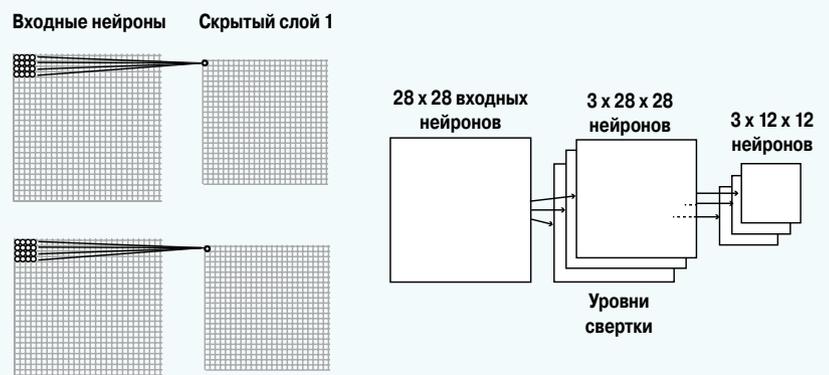


Рис. 4. Сверточная нейронная сеть ▲

Рис. 5. Петля обратной связи ▶

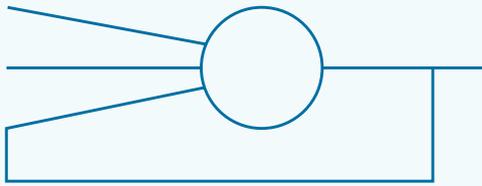


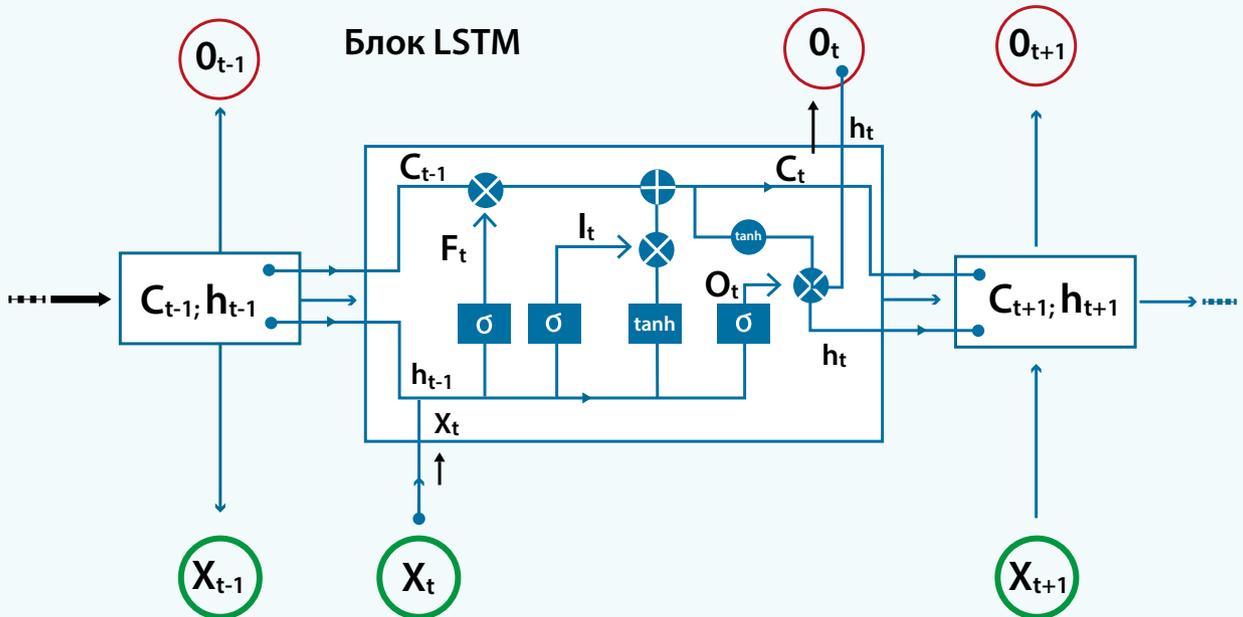
Рис. 6. Рекуррентная нейронная сеть ▼



Взгляните на основной блок. Закрашенные прямоугольники представляют собой целые слои, символ внутри которых обозначает вид функции активации (выход). Кружки с символами «×» и «+» представляют операции умножения и сложения соответственно. Посмотрите на первую комбинацию (выход слоя с сигмой умножается на выход предыдущего члена). Если этот уровень дает нулевое значение, то умножение фактически обнуляет предыдущий член. Другими словами, эта первая комбинация – схема забывания.

Для обработки естественного языка требуется гораздо больше, чем просто знание синтаксиса и значения отдельных слов. Как в предыдущем примере вам удалось узнать, что радуга содержит много разных цветов? Вы уже видели раду-

Рис. 7. Фрагмент сети LSTM ▶



Она позволяет обрабатывать последовательность элементов (например, слов в предложении), каждый из которых обеспечивает вход (или контекст) для последующих элементов.

Конечно, эта структура слишком проста, чтобы ее можно было использовать для обработки естественного языка, но более сложные нейронные сети с петлями обратной связи вполне для этого пригодны. Распространенный тип рекуррентной нейронной сети содержит так называемые блоки долгой краткосрочной памяти (Long Short-Term Memory, LSTM), как показано на рис. 7. Они хороши в запоминании слов (например, ключевого слова в предложении), а также способны «забывать» их при необходимости.

В этой сети можно найти определенное сходство с простой сетью на рис. 6, но здесь все гораздо интереснее.

гу и знаете, как она выглядит. И это общее знание контекста является третьим элементом обработки естественного языка (и самым сложным для компьютера).



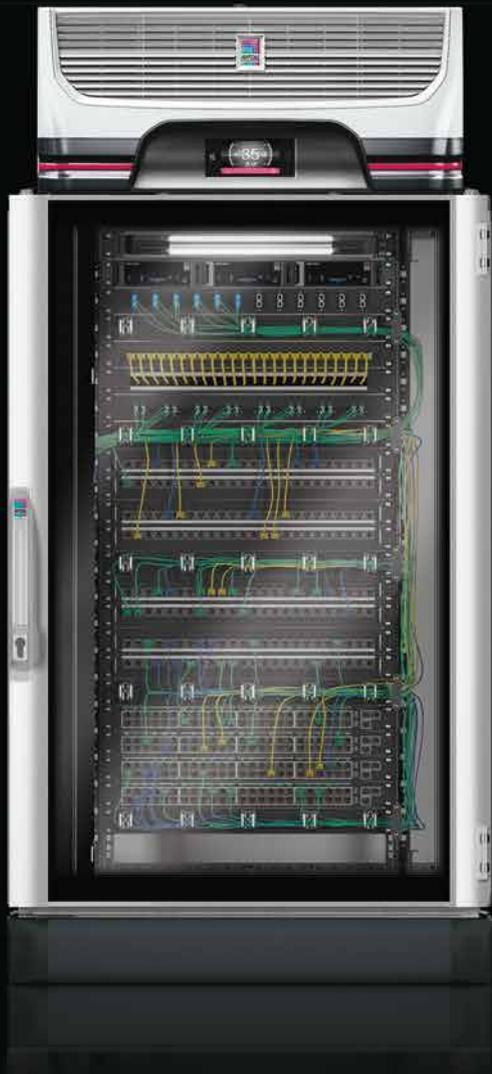
Есть множество других подходов к нейронным сетям, которые имеют различные сильные и слабые стороны или используются для решения иных задач. Но описанные понятия применимы и там. Нейронные сети построены из одних и тех же базовых элементов: нейронов (со смещением), входов (с весами) и выходов (функций активации с конкретными профилями). Эти элементы используются для создания различных или специализированных слоев и компонентов (как LSTM выше или в Oracle Database). В сочетании с петлями обратной связи и другими соединениями они образуют нейронную сеть. ИКС

Rittal – The System.

Faster – better – everywhere.

Discover the Edge.

IT-инфраструктура на промышленных объектах.



Бесперебойное функционирование
Надёжное хранение данных
Гибкое масштабирование
Физическая безопасность

Реклама

ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

IT INFRASTRUCTURE

SOFTWARE & SERVICES

FRIEDHELM LOH GROUP

www.rittal.ru



Гибридный охладитель JAEGGI – уникальное решение на рынке ЦОДов



Сочетание режимов сухого и влажного охлаждения обеспечивает охладителям JAEGGI высокую производительность при небольшой занимаемой площади и позволяет значительно снизить потребление электроэнергии и дорогостоящей воды, прошедшей водоподготовку.

Системы адиабатического охлаждения для своих наружных блоков стали предлагать многие производители. Прошедшая в прошлом году выставка ChillVenta-2018 наглядно продемонстрировала этот тренд. При этом производители наружных блоков идут двумя путями: устанавливают либо закрытые градирни, либо обычные драйкулеры, которые дополняются системами адиабатического охлаждения различного типа (от распыления воды с помощью форсунок до кассетных увлажнителей воздуха).

Компания HTS на конференции «ЦОД-2019» в Москве представила решение производителя JAEGGI (Швейцария), который запатентовал новую технологию гибридных охладителей. Это оборудование сочетает в себе преимущества закрытых градирен и сухих охладителей жидкости.

JAEGGI (входит в группу компаний Guentner) с 1992 г. имеет патент на гибридный сухой охладитель и уже более 20 лет работает в сфере технологий охлаждения центров обработки данных. На сегодняшний день успешно эксплуатируются более 3000 единиц оборудования производства JAEGGI.

Преимущества гибридного охладителя JAEGGI

Гибридный охладитель JAEGGI сочетает в своей конструкции элементы сухих охладителей и закрытых испарительных градирен. Таким образом, он соединяет в одном продукте достоинства сухого и влажного охлаждения. Режим

работы зависит от температуры наружного воздуха и от тепловой нагрузки в помещении дата-центра.

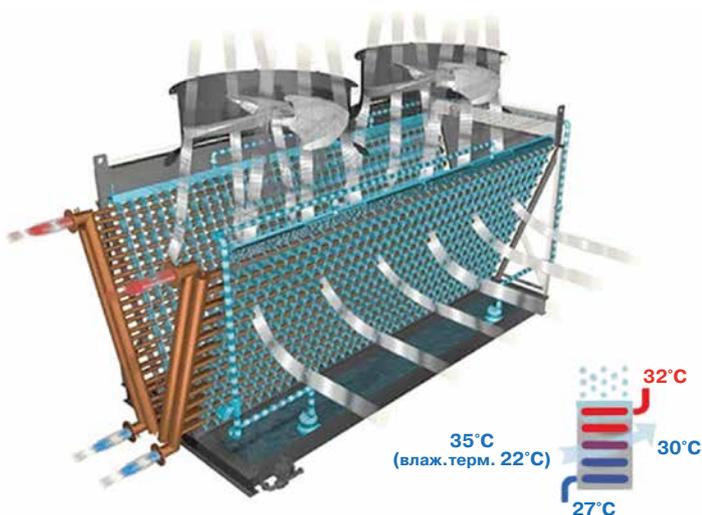
В числе преимуществ гибридного охладителя:

- энергоэффективность и низкий уровень потребления воды;
- отсутствие туманообразования и выброса аэрозоля;
- экономия эксплуатационных расходов;
- низкий уровень шума и компактность.

Градирня JAEGGI имеет закрытую конфигурацию. В режиме влажного охлаждения вода подается сверху на ламели не снаружи, а внутри аппарата, затем спускается по теплообменнику и попадает в специальный поддон, из которого при помощи насосов вновь поднимается наверх, и цикл повторяется.

Благодаря такому принципу работы потеря дорогостоящей воды, прошедшей предварительную водоподготовку, снижается на 70–90% по сравнению с аналогами, к примеру с традиционными градирнями, где вода распыляется на теплообменник в форме аэрозоля под давлением.

За счет конструкции охладителя JAEGGI в процессе работы не парят, не образуют луж и ржавчины. Вода в градирне обеззараживается при помощи ультрафиолетовых ламп, что позволяет избежать неприятных последствий: цветения, грибка, плесени и размножения бактерий. И при этом с одной градирни можно отводить до 3 МВт тепла.



▲ Схема работы гибридного охладителя JAEGGI

Гибридные охладители можно устанавливать в непосредственной близости с офисными зданиями – они имеют низкие шумовые характеристики, и в них отсутствует эффект парения в отличие от орошаемых градирен, аэрозоль от которых может поступать в открытые окна.

Градирни JAEGGI обеспечивают высокую производительность при небольшой занимаемой площади, а отсутствие форсунок, которые имеют свойство засоряться и требовать замены, позволяет снизить эксплуатационные затраты.

Что касается логистики, то гибридные градирни в стандартном исполнении могут поставляться в разобранном виде. Это большой плюс в тех случаях, когда на объект сложно заносить оборудование, например, если здание находится в центре города.

Оборудование JAEGGI уже давно и широко используется на целом ряде объектов, в числе которых самый «зеленый» ЦОД Equinix в Амстердаме, ЦОД оператора связи Swisscom, банк Credit Swiss, ЦОД Magdeburg (самый большой в Германии), DESY – немецкий исследовательский центр по физике частиц и другие компании с мировым именем.

JAEGGI в действии – ЦОД Swisscom

Дата-центр Swisscom (Берн-Ванкдорф, Швейцария) считается одним из самых энергоэффективных в Европе. Благодаря применению инновационных энергетических технологий в нем на охлаждение затрачивается на 90% меньше энергии, чем в дата-центрах с традиционным оборудованием. В ЦОДе установлен гибридный охладитель JAEGGI, основные характеристики которого приведены в таблице.

84% электроэнергии используется для ИТ-инфраструктуры и только около 4% идет на охлаждение и 4% на вентиляцию. Тепловая энергия, отводимая из центра обработки данных, подается в сеть централизованного теплоснабжения Берна и обеспечивает домохозяйства теплом и горячей водой, а также используется для подогрева открытого бассейна Wyler.

В ходе реализации проекта Swisscom превысила максимальную температуру воздуха в 27°C, рекомендованную

Основные характеристики системы охлаждения JAEGGI в ЦОДе Swisscom

Характеристика	Значение
Количество установок, шт.	8
Тепловая нагрузка, кВт	6 000
PUE	1,22
Хладоноситель	34%-ный гликоль
Расчетная температура хладоносителя, °C	35/25
Рабочий режим градирни:	
Сухой, температура воздуха на входе, °C	14,9
Гибридный, температура/влажность воздуха на входе, °C/%	32/38*
Общий расход воды (испарение), м³/ч	13,8 на 8 установок

* Соответствует температуре влажного термометра (на входе) 20,9°C.

ASHRAE для центров обработки данных. ИТ-инфраструктура в ЦОДе Swisscom рассчитана на максимально допустимую температуру +28°C, и даже в течение нескольких часов возможно повышение температуры до +32°C.

В Swisscom смогли добиться значения PUE, равного 1,22 (при среднем европейском значении 1,9), благодаря отказу от традиционных холодильных машин в пользу гибридного охлаждения JAEGGI.

Swisscom использует свободное охлаждение при помощи восьми гибридных градирен JAEGGI, чтобы максимально снизить потребление электроэнергии. В зависимости от требуемой тепловой нагрузки свободное воздушное охлаждение дополнительно поддерживается за счет испарения воды, начиная с температуры воздуха около 21°C. Испаряемая вода используется для охлаждения проходящего через теплообменник потока хладоносителя. Пока орошение не активировано, для рассеивания тепловой энергии достаточно непрерывной работы вентиляторов. Орошение активируется автоматически собственным контроллером установки в зависимости от требуемой мощности охлаждения. Интегрированная система управления и регулирования устанавливает минимальную скорость вращения вентиляторов, достаточную для отведения тепловой нагрузки. Дождевая вода хранится в контейнере емкостью около 2000 м³ и используется для орошения гибридных охладителей.

В России дистрибьютором гибридных охладителей JAEGGI является компания HTS, которая уже на протяжении многих лет сотрудничает с компанией Guentner и реализовала множество проектов на базе оборудования одного из ведущих европейских производителей.



www.h-ts.ru

IX-вектор в эволюции ЦОДов

Андрей Перекрест,
руководитель
московского
ЦОДа,
Linxdatacenter

Развитие цифровой экономики меняет привычные роли игроков в ИТ-сфере. ЦОДы уже стали многофункциональными сервис-провайдерами. Сегодня на рынке появляется новый тренд: ЦОДы все чаще берут на себя функции точек обмена трафиком – IX-узлов.

Площадки обмена трафиком (Internet Exchange Point, IX) первоначально возникали в крупных мировых городах с выгодным с точки зрения маршрутизации трафика расположением: во Франкфурте, Лондоне, Амстердаме, Стокгольме, Москве и т.д. В российской столице первая IX-площадка появилась в 1995 г. на Московской междугородной телефонной станции № 9. В такие точки по всему миру сходятся магистральные каналы связи для дальнейшей маршрутизации по различным направлениям.

Сегодня в России работают несколько десятков IX-точек. Все они играют важную роль в структуре Рунета, а многие дата-центры на базе ресурсов IX оказывают своим клиентам услуги организации соединительных линий в рамках сервисов meet-me-room.

Ключевой элемент глобальной сети

IX сегодня – это хабы с высочайшей концентрацией всех существующих сетевых ресурсов, от сетей любого профиля и корневых DNS-серверов до различных сервисных платформ (GRX, eNum, VoIP), частных и публичных облаков и т.д.

Присутствие компании в ключевой региональной IX-точке позволяет ей в короткие сроки организовать качественное взаимодействие с потребителями своих ресурсов на нужном географическом пространстве. Этот эффект достигается за счет пиринга – прямого взаимодействия

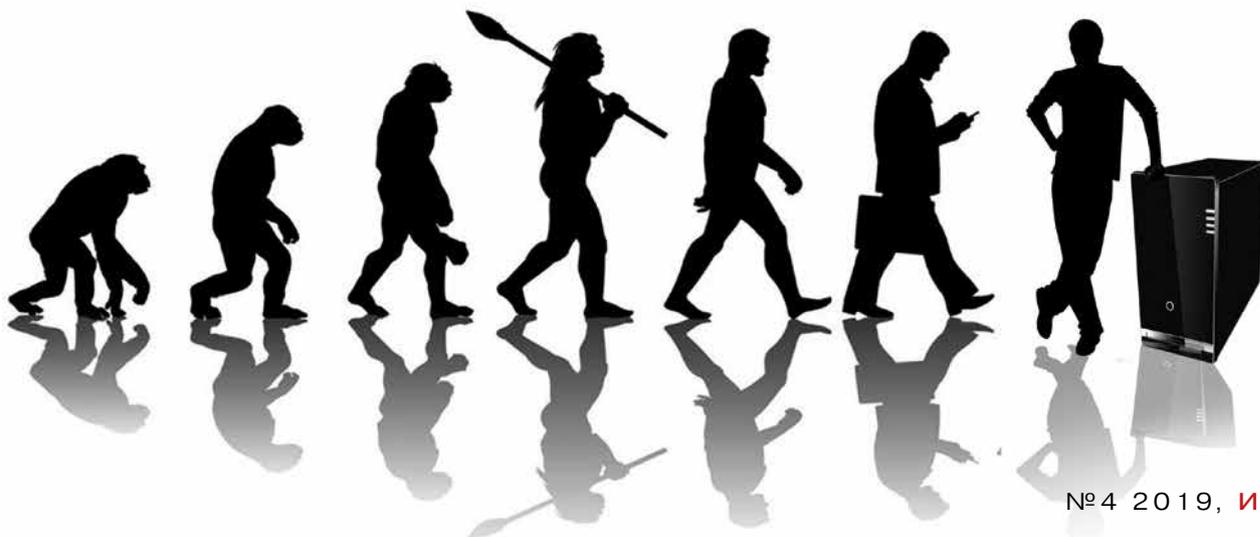
самых разных сетей с минимальными задержками и потерями. Подсети глобальной сети, сети доставки контента и облачных сервисов – все они работают в рамках открытой пиринговой политики для уменьшения сложностей в процессе доставки данных и контента до конечного пользователя.

IX-площадки в целом повышают доступность сетевых ресурсов, увеличивают скорость соединения и передачи данных, снижают стоимость трафика из-за сокращения маршрута передачи данных и дают возможность нескольким операторам разделять издержки на обслуживание инфраструктуры. Для небольших провайдеров упрощаются подключение и доступ к готовой инфраструктуре.

Больше чем ЦОД

Как сегодня эволюционируют IX-узлы и их возможности?

На крупные IX-площадки приходит все больше клиентов, объем трафика растет по экспоненте, что приводит к его частичному перенаправлению с привычных маршрутов на площадки прямого обмена, в том числе в дата-центрах. За счет доступа к ресурсам IX-площадок и каналам прямого соединения с крупнейшими облачными платформами, которые нужны компаниям для развития бизнеса, дата-центры уже сами по себе могут выступать в качестве операторов связи.



Возможности дата-центров в плане ИТ-инфраструктуры и точек обмена трафиком в части связности (connectivity) идеально дополняют друг друга, в результате чего бизнес-клиенты ЦОДов могут получать синергический эффект от размещения своих ресурсов на площадках с расширенным IX-функционалом. Доступ ЦОДов к ресурсам IX позволяет обеспечить подключение к любой сети мира в кратчайшие сроки. Для бизнеса это важно, поскольку качество связности напрямую влияет на скорость работы приложений, обмен данными с контрагентами, пользователями и т.д.

Обмен потоками B2B-трафика в обход каналов крупных магистральных операторов связи обеспечивает отсутствие задержек и потерь при передаче информации, прямую связность с необходимыми ресурсами, легкость масштабирования и управления любыми параметрами. Так, скорость обмена трафиком зависит от многих факторов, но если обмен осуществляется локально и напрямую между двумя сторонами в ЦОДе, то по сути стороны взаимодействуют через свой собственный интернет. Никаких потерь, задержек, рисков сбоя, возникающих у операторов связи и сторонних IX. Традиционный интернет, конечно, нужен и при таком подходе, но небольшим операторам и корпоративным клиентам сегодня становится выгоднее стыковаться напрямую через подобные платформы, без участия третьих лиц.

Возможность прямого обмена трафиком в дата-центре позволяет сегодня оптимально решать задачи объединения любых облачных платформ и физической инфраструктуры бизнеса. Например, при развертывании ИТ-систем с гибридной архитектурой, включающей собственные on-premise и облачные компоненты, ресурсы стороннего оператора связи, части ИТ-инфраструктуры партнеров, общая связность решения оптимальным образом обеспечивается именно через IX-платформу в ЦОДе.

Типичный пример: контент-провайдеру нужно подключиться к большому количеству операторов связи, к партнерским компаниям, оказывающим услуги в области информационной безопасности и различные дополнительные услуги. У каждого из этих партнеров и операторов есть своя сетевая инфраструктура, свои настройки и другие переменные – все это нужно связать, синхронизировать, обеспечить точечную настройку каждого узла, порта, канала связи. Это огромная работа, по сути – отдельный проект.

Если же все стороны подобного взаимодействия присутствуют в одном ЦОДе, у которого есть собственная IX-платформа, то участники проекта пользуются единой точкой входа и при-



соединения. Тогда по принципу одного окна помимо технологических задач решается и любой вопрос, связанный с коммерческими аспектами, техподдержкой и т.д.

При этом выбор всегда остается: можно тянуть канал до магистральной линии, «коннектиться» с каждым партнером отдельно, неся все инфраструктурные издержки и риски, но при наличии IX-платформы в ЦОДе разумнее подключиться к ней, существенно сократив свои затраты и снизив риски.

Рынок постепенно приходит именно к такой модели. Подобные решения становятся нормой для коммерческих дата-центров во всем мире, включая Россию.

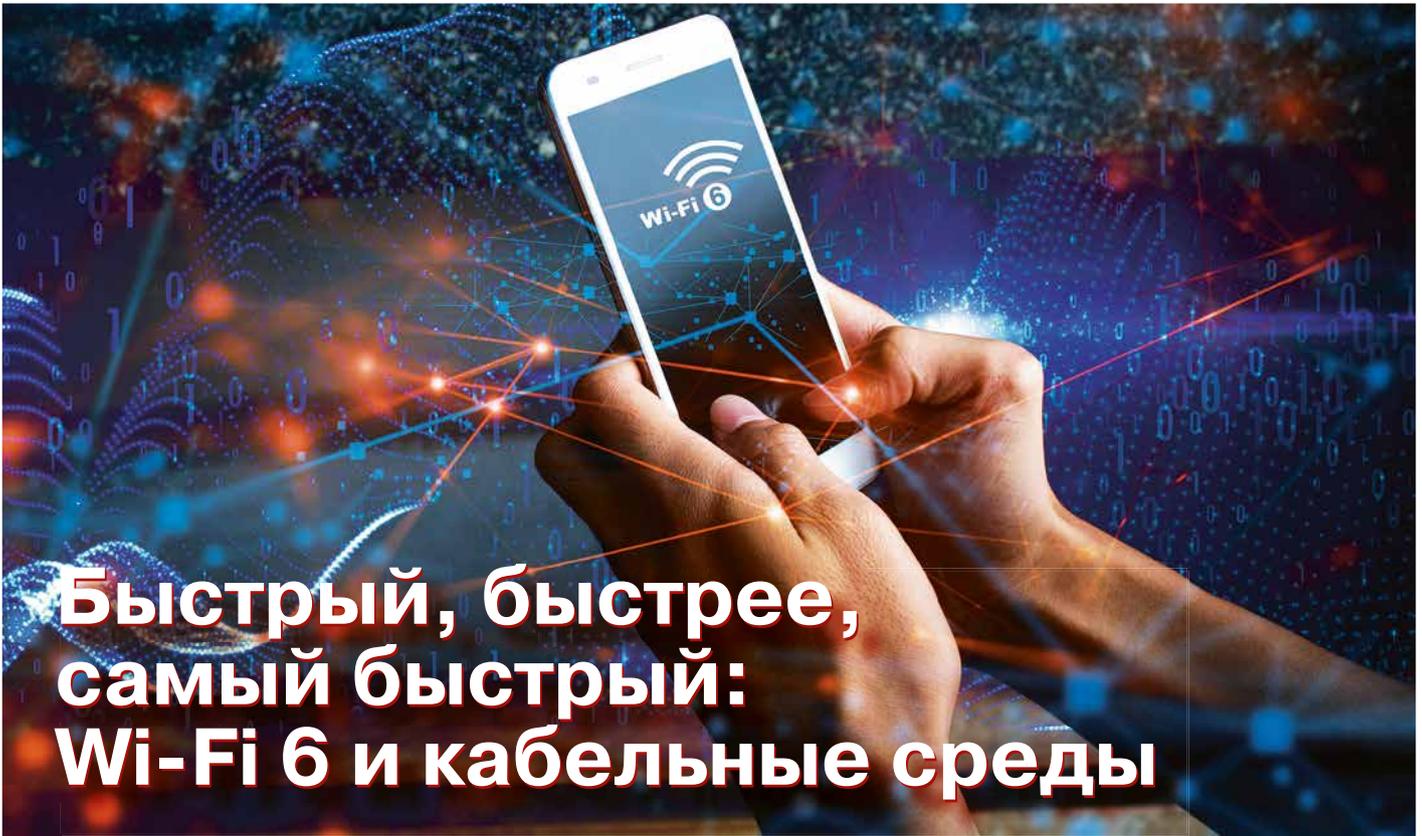
IX как новая ниша для дата-центров

Приведет ли новый тренд к прямой конкуренции классических IX-точек и дата-центров за трафик?

На мой взгляд, нет. Появление IX-функционала в ЦОДах не станет для их бизнес-модели коммерческим прорывом. Для ЦОДов такое расширение собственных компетенций – лишь очередной виток наращивания портфолио сервисов, логическое развитие сетевого направления в целом для решения определенного класса локальных задач клиентов, т.е. освоение новой ниши на рынке комплексных ИКТ-услуг.

Кроме того, включение в свой инструментарий возможностей IX-точек позволит дата-центрам развивать свои компетенции в соответствии с усложнением сетевой инфраструктуры современных компаний. Этот процесс сегодня подразумевает использование удаленных площадок и их ресурсов, облаков всех видов и конфигураций для масштабирования, а также резервирования данных и приложений.

Если прибавить к этому стремительный рост потребностей в обеспечении отказоустойчивости сети и защиты от потери данных, то IX-вектор для ЦОДов становится чуть ли не главным в плане развития сетевого направления. **ИКС**



Быстрый, быстрее, самый быстрый: Wi-Fi 6 и кабельные среды

Николай Ефимов,
технический
менеджер,
Siemon

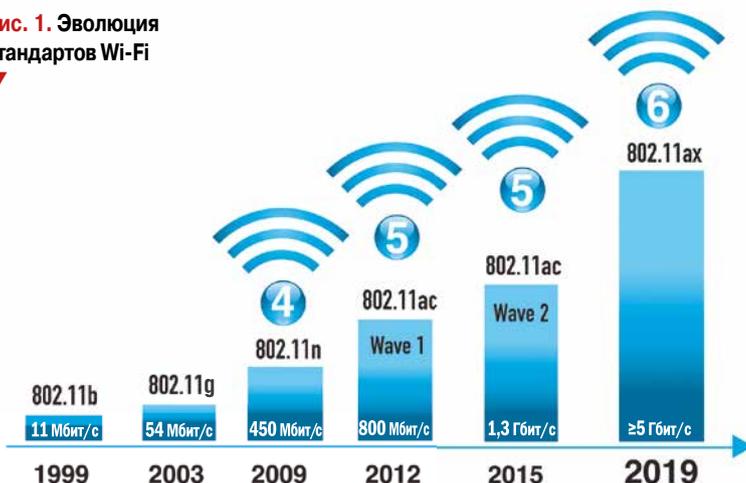
Чтобы потенциал беспроводных решений Wi-Fi 6 раскрылся полностью, кабельная система, к которой подключаются точки доступа, должна быть правильно спроектирована и инсталлирована. При этом важно учесть ряд факторов, включая дистанционную подачу электропитания.

Люди используют все больше мобильных и портативных устройств – смартфонов, планшетов, ноутбуков. Для поддержки бизнес-приложений, просмотра видео Ultra HD и мультимедийного контента им все чаще требуется быстрая работа Wi-Fi. Для этого к локальной сети нужно подключить производительное беспроводное оборудование и следить за тем, чтобы в системе не было узких мест. Итоговая система должна быть высокопроизводительной и обе-

спечивать быстрый отклик. Новое поколение технологий, известное как Wi-Fi 6 (802.11ax), существенно увеличивает пропускную способность беспроводных систем и поддерживает скорости свыше 5 Гбит/с. Растут пропускная способность, производительность систем, плотность устройств в зоне обслуживания; уменьшается время отклика; увеличивается время работы аккумуляторных батарей.

Полностью раскрыть потенциал беспроводных решений Wi-Fi 6 можно лишь тогда, когда кабельная система, к которой подключаются точки доступа, правильно спроектирована и установлена. При проектировании кабельной системы и выборе среды передачи для подключения беспроводного оборудования Wi-Fi 6 необходимо учитывать целый ряд факторов.

Рис. 1. Эволюция стандартов Wi-Fi



Поддержка высоких скоростей Wi-Fi

Технология Wi-Fi 6 поддерживает скорости свыше 5 Гбит/с (рис. 1), и это существенно сужает выбор возможных сред для кабельных сегментов между узлами сети. В точках доступа WAP (Wireless Access Point), выполненных по технологии Wi-Fi 6, для подключения к сети Ethernet используется не один порт, как раньше, а два,

причем как минимум один из них должен поддерживать скорость 2,5 или 5 Гбит/с. По мере того как технологии Wi-Fi 6 будут развиваться, возникнет потребность в поддержке скоростей свыше 5 Гбит/с. Если существующая кабельная инфраструктура не обеспечивает 10-гигабитных скоростей передачи, то для одной точки доступа Wi-Fi 6 необходимы минимум два 5-гигабитных подключения. При этом уже просматривается будущая потребность в двух 10-гигабитных подключениях, ведь беспроводные технологии продолжают совершенствоваться.

Все это означает, что в системе будет использоваться высокопроизводительное активное оборудование, а кабельная среда передачи должна обеспечить пропускную способность не менее 10 Гбит/с – либо по витой паре, либо по многомодовому оптическому волокну, причем как в горизонтальных подсистемах, так и в магистрях. В ином случае реализовать беспроводные приложения Wi-Fi 6 не удастся.

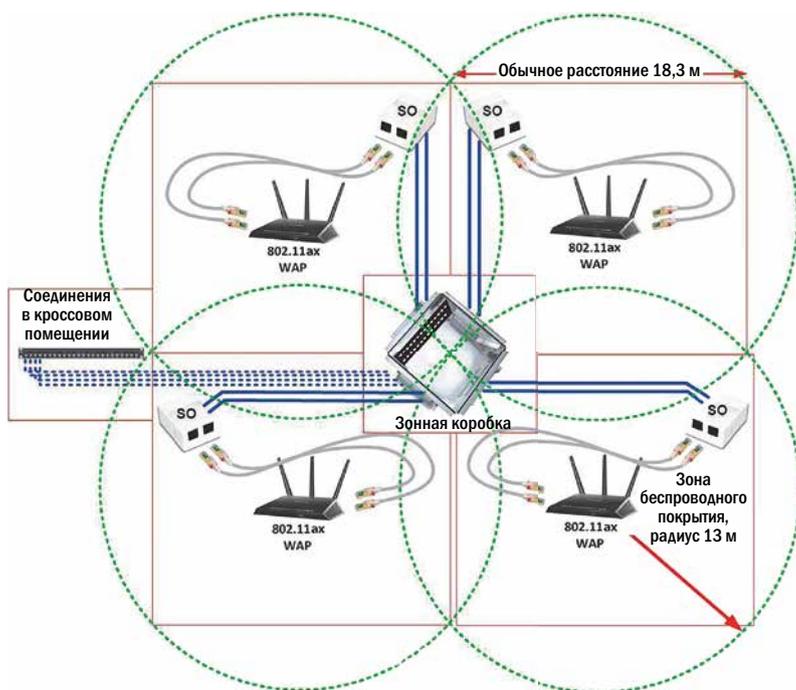
К каждой точке доступа WAP Wi-Fi 6 следует подводить по два кабельных сегмента класса EA/категории 6A, рассчитывая на подключение к двум портам Ethernet, – только так можно обеспечить необходимую скорость передачи для различных конфигураций устройств.

Запитывание устройств Wi-Fi 6

Еще один важный аспект – подведение питания к беспроводной точке доступа, выполненной по технологии Wi-Fi 6. Обработка сигналов радиочипами Wi-Fi 6 гораздо сложнее, чем в оборудовании предшествующих поколений, для нее требуется более мощное питание. Каждой точке доступа Wi-Fi 6 необходимо обеспечить либо локальное подключение к источнику постоянного тока, либо удаленное питание PoE Type 2 мощностью 30 Вт. Но при удаленном запитывании по PoE Type 2 каждая пара несет ток 600 мА, что вызывает нагрев кабельного пучка. Повышение температуры может достигать 10°C в сравнении с температурой окружающей среды. Нагрев сопровождается увеличением числа битовых ошибок, что ведет к снижению производительности. Кроме того, при отключении оборудования «по-живому» возникает электродуговой разряд, что со временем приводит к выгоранию контактов на коннекторах и в портах.

При выборе кабельной среды настоятельно рекомендуется отдавать предпочтение экранированным кабельным решениям, поскольку они устойчивы к повышению температуры, характерному для приложений PoE. Следует выбирать кабельные системы, которые обеспечивают надежную работу и механическую прочность при температуре до 75°C – именно они способны поддержать подачу питания PoE Type 2 и функционирование во всем диапазоне рабочей температуры – от -20°C до 60°C. Экранированные кабельные решения категорий 6A и 7A демонстрируют наибольшую стой-

ПОДВЕДЕНИЕ ПИТАНИЯ К Точкам доступа Wi-Fi 6



▲ Рис. 2.
Зональная
архитектура
сети Wi-Fi 6

кость к нагреву и в таких условиях поддерживают передачу в каналах большей протяженности. Подобные системы позволяют увязывать в пучки больше кабелей без превышения допустимого прироста температуры. Кроме того, применение коммутационного оборудования, соответствующего стандарту IEC 60512-99-001, обеспечит долгий срок службы контактов и предотвратит повреждение вилок и портов при отключении оборудования «по-живому», когда в системе используется довольно мощное удаленное питание Wi-Fi 5 и Wi-Fi 6.

Гибкость при проектировании и размещении точек доступа WAP

При создании кабельной инфраструктуры для надежной поддержки решений Wi-Fi 6 нужно учитывать скорости подключения сетевых коммутаторов, серверов и устройств, доступных сегодня на рынке, а также стратегии их обновления, развития будущих беспроводных технологий и обеспечения надежной работы систем.

Кабельные системы класса EA/категории 6A, построенные на основе зонального подхода и точек концентрации сервисов (SCP) в зонных шкафчиках, обеспечивают нужную плотность портов и поддержку приложений 2,5/5GBASE-T в расчете на каждую точку доступа WAP. Те же системы гарантируют эффективное использование портов при подключении оборудования 10GBASE-T в будущем.

Зональный подход обеспечивает необходимую гибкость и позволяет легко менять конфигурацию в зонах обслуживания. Для него характерны наличие запаса и учет потребностей бу-

дущих технологий, в том числе использование нескольких сегментов 10GBASE-T для подключения устройств. В существующую беспроводную сеть всегда можно добавить точки доступа WAP, чтобы улучшить покрытие. Это практически не доставит неудобств обитателям здания, поскольку в зонных подсистемах всегда есть резервные порты. Эксперты компании Siemon рекомендуют, чтобы каждый зонный шкафчик обслуживал зону радиусом 13 м (рис. 2). Количество портов (кабельных окончаний) в точке концентрации сервисов варьируется от 24 до 96 в зависимости от офисной или иной среды в здании, принятого уровня автоматизации, типа потолочного освещения, вида и количества приложений – Wi-Fi, системы безопасности, видеонаблюдения, контроля доступа, другого оборудования автоматизации здания. Взаимное расположение точек SCP может основываться на сетчатой структуре, конфигурации для протяженных сегментов или структуре из шестиугольников.

Там, где к системе подключается стационарно расположенное оборудование, можно оконцовывать кабельные сегменты вилками категории 6A для полевой заделки. Это дополнительно упрощает установку точек доступа WAP, избавляет от необходимости точно указывать длину сегмента, держать запас коммутационных шнуров определенной длины, заказывать шнуры с оболочкой в пленумном исполнении и решать, где и как уложить запас кабеля около точки доступа WAP. При терминировании сегментов в полевых условиях рекомендуется использовать конфигурации канала с минимум двумя точками соединения, поскольку это обеспечивает необходимую гибкость и удобство внесения изменений в систему, добавления и удаления кабелей, облегчает полевое тестирование системы, маркировку портов и кабельных окончаний.

■ ■ ■

Решения Wi-Fi развиваются, в них достигаются скорости передачи свыше 5 Гбит/с. Для их реализации требуются мультигигабитные кабельные системы и удаленное питание PoE Type 2. Чтобы добиться оптимальных характеристик сетей, проектировщики, монтажники, консультанты и конечные пользователи не должны упускать из виду кабельную инфраструктуру, к которой подключается беспроводное оборудование. Только грамотно спроектированная и установленная кабельная система на основе экранированных кабелей класса EA/категории 6A или выше, стойких к повышению температуры, обеспечит надежную поддержку беспроводных технологий Wi-Fi 6 и будущих беспроводных приложений. ИКС

Языки HTML/CSS, Shell и SQL используются широко, но в качестве вспомогательных. Главной специализацией они являются лишь для небольшого числа программистов.

Python и Java: номер два по факту с большим потенциалом роста

Несмотря на формальные позиции в рейтинге с номерами 4 и 5, языки Python и Java по факту делят второе место по популярности в качестве инструмента написания кода.

Python – в высшей степени удобный для пользователя язык, интуитивно понятный, обладающий прозрачным синтаксисом. Некоторые даже сравнивают его с естественными языками, например с английским.

По данным Stack Overflow, Python наиболее часто рассматривается в плане освоения в качестве второго языка с перспективой полного перехода на него: 12% опрошенных разработчиков планируют такой переход в ближайшее время, что на сегодня является наивысшим показателем. По версии исследования JetBrains, эта цифра еще выше – 27% респондентов начали или продолжили его изучение за последние 12 месяцев.

Python отлично подходит для back-end-разработки, предоставляет широкий спектр возможностей и широко распространен в самых разных отраслях и работающих там приложениях. Еще одна причина всплеска популярности языка – его высокая применимость в задачах, связанных с такими областями современного хай-тека, как машинное обучение, нейросети и обработка больших массивов данных (data science).

Python поддерживает написание кода, сочетающее использование простых функций и переменных без акцента на определения класса.

Что касается Java, то этот язык – один из самых востребованных в последние 20 лет. Это объектно-ориентированный язык, более простой, чем C++, за счет наличия автоматического распределения памяти и сбора мусорного кода. Java также один из наиболее платформо-независимых языков. Писать на нем можно с помощью любого устройства, далее скомпилировать его в низкоуровневый машинный код, а затем выполнить его на любой платформе с помощью виртуальной Java-машины (JVM).

Сегодня Java является базой для ОС Android и применяется в практике 90% компаний списка Fortune 500 для широкого спектра back-end-приложений. Язык остается одним из лидеров в роли единственного используемого программистом языка – 44%, по данным исследования JetBrains.

Семейство C и PHP: старые кони для новых борозд

C – один из самых старых языков в мире. Он остается востребованным и по-прежнему вно-

сит существенный вклад в отрасль программирования, являясь корневым для целого семейства: Java, Objective-C, C# и C++.

Незаменимый инструмент для разработки высокопроизводительных систем, C также является базой для OS Linux и оптимальным выбором для создания верхнеуровневых приложений. C++ часто выбирают разработчики игр, создатели VR-решений, также он подходит для всего комплекса задач, связанных с графикой. Распространенность и популярность C-языков очевидна из рейтинга.

То, что создавалось в 1994 г. как набор инструментов для развития и поддержки личной страницы программиста, теперь используется в 83% всех веб-сайтов в интернете. Язык PHP предназначен для создания веб-страниц на HTML: бесплатный, простой в настройке и освоении начинающими программистами, он сверхпопулярен, особенно для создания динамического контента веб-страниц.

Вне топа не значит «аутсайдер»

Отставание от первой десятки в таких рейтингах вовсе не означает невостребованность или неактуальность: множество ситуативных факторов могут влиять на позиции языка программирования в текущий момент, что видно по некоторым участникам топ-10, попавшим туда относительно недавно.

В ближайшем арьергарде следует отметить Swift как базовый язык для разработки всего, что связано с Apple (iOS и Mac OS). На него повлияли Python и Ruby, он более быстрый и защищенный, чем считающийся его предшественником Objective-C. Swift подходит для новичков и требует меньше кода, больше напоминая естественный язык. На него просто переключаться тем, кто владеет JavaScript, Java, Python, C# и C++. Тем не менее Swift отличается сравнительно небольшим количеством компетентных разработчиков – только 8,1% сообщества использует его в качестве главного языка, а из-за частоты обновлений Swift также считается менее стабильным с каждым новым релизом.

Язык Ruby родом из Японии. Это динамичный open source-язык программирования, сфокусированный на простоте использования и высокой продуктивности. Нетребователен к количеству строчек кода, больше походит на естественные языки и служит для разработки простых приложений. Сложности, ограничивающие его применимость, заключаются в самой природе Ruby – динамически типизированный язык непросто поддерживать, а его гибкость делает его довольно медленным инструментом.

SQL широко используется для всех задач, связанных с базами данных в веб-фреймворках и

БД-приложениях. Владение SQL позволяет оптимизировать управление процессами анализа данных и улучшать качество решений, принимаемых на основе этой информации. SQL-девелоперы всегда ценились высоко, а с ростом роли данных в современных digital-проектах этот тренд становится еще более явным.

Данные исследования JetBrains также ставят в перечень наиболее перспективных для изучения в будущем язык Go: сегодня его используют всего 18% разработчиков (8% в прошлом году), однако сразу 13% назвали Go целью своего обучения и дальнейшей миграции в следующем году. Язык предназначался для создания высокоэффективных программ, работающих на современных распределенных системах и многоядерных процессорах. Go – продукт компании Google, поэтому в перспективах развития сомневаться не приходится.

Что учить?

Тема языков программирования – одна из самых актуальных в HR-среде рынка ИТ.

К сожалению, российский рынок ИТ в целом и его кадровая составляющая в области разработки в частности таковы, что гарантировать долгосрочную перспективу стабильного развития карьеры при владении одним языком невозможно. Как мы видим, одни языки довольно долго остаются в обойме, роль многих заметно уменьшается со временем, а другие «выстреливают» благодаря разнообразным естественным рыночным и отраслевым факторам.

В России к естественным факторам добавляется влияние государства на развитие ИТ-рынка. Скажем, по каким-то причинам госзаказ в области ИТ отказывается от использования C-семейства в своих разработках, а привилегии получает язык, не входящий сегодня и в топ-30. С другой стороны, в нашей стране государственным решением может быть создан массовый спрос на довольно продвинутые технологии, причем выбор будет сделан в пользу самых све-

жих технических решений. Что, в свою очередь, создаст спрос на специалистов в этой области.

Но и на Западе в этом отношении тоже не все просто. В целом традиция защищать свои инвестиции в ИТ в долгосрочной перспективе и пестовать специалистов, компетентных в определенном технологическом стеке (включая язык), там развита сильнее, чем у нас. Однако и там в рынок вмешивается множество случайных факторов – возьмите историю с языком Kotlin наших разработчиков из JetBrains. Нельзя сказать, чтобы он обладал какими-нибудь уникальными возможностями, но в нужный момент времени показался менеджерам Google вполне убедительным (особенно в свете трений компании с Oracle по поводу использования Java), и был принят в состав Android Studio 3.0, официального инструмента разработки для ОС Android.

Еще один момент: популярность языка не определяется его удобством или внутренними качествами. C++ – переусложненный, неудобный язык. С точки зрения функциональности его востребованность не объяснить. Java задумывался как язык для устройств и «выстрелил» за счет скачка веб-разработки в начале 2000-х гг. Расцвет Python мы видим только благодаря прорыву больших данных и нейросетей. Предсказать, что будет следующим в этом списке, невозможно.

С другой стороны, давно существует весьма качественный язык D (это C++ без всех его основных минусов), но уровень его популярности по сравнению с лидерами практически нулевой. Драйверами успешности языка являются не его качества, а традиции использования, размер сообщества разработчиков и маркетинг. Продвигнуть новый язык сегодня и в будущем понастоящему смогут только ИТ-гиганты.

Что касается будущего спроса на языки, уверенным можно быть только в перспективах семейства C и Java – они будут востребованы за счет глубины проникновения в enterprise-сегмент, а также инерции сообщества разработчиков и экономики в целом. ИКС



**Специальные условия
при оформлении подписки для
корпоративных клиентов!**

Оформляйте подписку

в редакции – по телефону: +7 (495) 150-6424

или по e-mail: podpiska@iksmedia.ru

ИнформКурьер-Связь

ИКС

издается с 1992 года



Грани PaaS

Николай Носов

Сервисы PaaS все чаще используются компаниями для получения конкурентных преимуществ и успешного продвижения на рынке.

Разработчик зачастую создает решение не с нуля, а опирается на опыт предшественников. Нет смысла «изобретать велосипед», лучше взять уже проверенные, работающие решения, подстроить для своих задач и добавить что-то новое. Все это справедливо и в отношении программирования с использованием программных платформ – совокупности отработанных технологий и программ, позволяющих в реальные сроки создавать новые продукты путем настройки готовых решений и разработки дополнительных модулей, реализующих необходимый функционал.

С появлением облачных вычислений программные платформы переместились в облако и стали предлагаться по сервисной модели. Появился термин Platform as a Service (PaaS). Облачные платформы предоставляют возможность автоматической интеграции, согласования и развертывания систем; большой выбор средств разработки и API; широкий спектр шаблонов и готовых приложений, которые можно встраивать в создаваемое решение.

Пионеры PaaS

Включающий элементы PaaS сервис Amazon Elastic Compute Cloud (Amazon EC2) компания Amazon запустила еще в 2006 г., в 2008 г. заработали популярные PaaS Heroku и Google App Engine, ориентированные на конкретные стеки технологий (Ruby и Python соответственно). В том же году появилось первое программное обеспечение с открытым исходным кодом для развертывания частных и гибридных облаков – OpenNebula NASA. Проект позиционировался как IaaS, но включал и элементы PaaS.

К 2011 г. рынок публичных PaaS оценивался в \$700 млн, к числу крупнейших провайдеров относились Amazon.com (Beanstalk), Salesforce.com (Force.com, Heroku, Database.com), LongJump, Microsoft (Windows Azure), IBM (Bluemix), Red Hat (OpenShift), VMware (Cloud Foundry) и Google (App Engine).

PaaS-контейнеризация

Новым этапом в развитии PaaS стало использование контейнерной виртуализации, которая решает серьезную проблему разработчиков – привязку к платформе разработки. Контейнер – это автономно исполняемый фрагмент программного кода, который включает всё, что нужно для его запуска: собственно код, среду выполнения, системные инструменты, библиотеки, установочные файлы.

Размещение программы с требуемым окружением в контейнере позволяет безболезненно переносить решения, созданные в облаке, в корпоративную систему заказчика, «отвязывает» разработчи-

ка от конкретной облачной платформы и обеспечивает миграцию решений между облаками.

Контейнеры позволяют менять версии ПО «на ходу», не прерывая бизнес-процессов. Подход можно проиллюстрировать на следующем примере. Старая версия приложения работает в одном контейнере. В это время новая версия проверяется во втором контейнере, причем используется полностью идентичное окружение, что минимизирует число ошибок при последующем переходе. Примечательно, что сама эта новая версия может содержать обновленный код не только приложения, но и любых его зависимостей, а также системных компонентов (например, новую версию OpenSSL или всего дистрибутива). Когда новая версия полностью готова к обслуживанию запросов, трафик переключается с первого контейнера на второй, и старая версия может быть остановлена.

На практике в сервисе могут одновременно работать тысячи контейнеров, но сам принцип остается прежним – версия ПО меняется постепенной заменой контейнеров на новые. При необходимости можно легко осуществить откат к предыдущей версии (достаточно переключить трафик на старые контейнеры).

В 2018 г. объем глобального рынка контейнеров приложений достиг \$1,5 млрд. По оценкам Grand View Research, в 2019–2025 гг. CAGR составит 26,5%, причем в облачном сегменте (по прогнозу, в 2025 г. на него будет приходиться 45% рынка) рост будет еще больше – около 30%.

Контейнеризация вдохнула в PaaS новую жизнь и сформировала современный облик платформенных сервисов. В настоящее время PaaS является наиболее динамично растущим сегментом облачного рынка.

Классификация PaaS

Прикладные программисты пользуются платформой разработки приложений aPaaS (Application Platform as a Service), которые постоянно развиваются. Общая тенденция развития ИТ – упрощение труда программиста: автоматизация средств написания кода, возможность создания решений на высоком уровне, в идеале – любым пользователем, не владеющим навыками программирования. Первые системы такого рода стали применяться еще в 80-х, когда появились CASE-системы: программист рисовал блок-схему программы, а CASE-система генерировала код. Развитие подхода привело к появлению рынка платформ с низким использованием кода – low-code/no-code в терминологии Forrester, или HPaaS (High Productivity Application Platform as a Service) в терминологии Gartner.

Low-code-системы можно разделить на системы генерации исполняемого кода и создания мо-



Ли Майлз, региональный менеджер по Центральной Европе, СНГ, Среднему Востоку и Африке, Red Hat

Корпоративный пользователь хочет иметь платформу для разработок, но не хочет заниматься ее настройкой и сопровождением. Именно в этот момент на сцену выходит PaaS.

дели представления (Model-Driven Execution Platform).

Поставщики систем генерации исполняемого кода предоставляют визуальную среду разработки приложений. Преимущество подхода – возможность генерации кода приложений, работающих без доступа к интернету. Это в общем случае дает возможность создавать приложения с более высокой производительностью. Независимость полученного кода от платформы – большой плюс в случае проблем с платформой, ведь ее поставщик может по тем или иным причинам уйти с рынка. Поставщики таких решений – компании OutSystems, Alpha Software, AppGyver, Graphite GTC, Kuika, Lansa, OrangeGrid, Progress Kinvey, Vantiq и Zuznow.

Другие поставщики применяют подход на основе модели представления. В этом случае генерируется промежуточное представление разрабатываемого приложения, которое платформа интерпретирует непосредственно во время выполнения. Подобные решения предлагают Salesforce, ServiceNow и Mendix, а также Appian, Betty Blocks. Model-Driven Execution Platform хорошо подходит для реализации мобильных веб-приложений, которые работают в браузерах на мобильном устройстве. Еще один плюс – независимость от обновлений платформы, устанавливаемых провайдером.

Набирают популярность бессерверные вычисления (Serverless computing) – использование конкретных функций в облаке, при котором облачная платформа динамично руководит выделением машинных ресурсов, по сути, для каждого запроса создает отдельный контейнер, который уничтожается после выполнения. А пользователь оплачивает конкретное «полезное действие». Наиболее популярные примеры – AWS Lambda, Azure Functions.

Упрощение написания программ размывает границы между PaaS и SaaS. Все чаще конечный пользователь может получить нужное решение самостоятельно, не прибегая к услугам программистов, а разработчики – использовать в качестве платформы разработки классические решения SaaS, например Microsoft Excel.

С ростом числа облачных сервисов, приложений и платформ выросло и разнообразие API, обеспечивающих обмен данными. На их интеграцию и поддержку стало требоваться много

ресурсов разработчиков. Для сглаживания этих проблем появились интеграционные платформенные сервисы – Integration Platform as a Service (iPaaS) – наборы облачных сервисов, которые позволяют разрабатывать, интегрировать и обслуживать потоки, соединяющие различные локальные и облачные сервисы, процессы, приложения и данные внутри одной или нескольких организаций.

Основные свойства iPaaS: простота разворачивания системы, наличие готовых коннекторов к популярным приложениям и сервисам, пакеты для их быстрой разработки, графический, не требующий программирования интерфейс, обработка ошибок с уведомлением по e-mail. Предлагают такие платформы компании Infomatica, Dell Boomi, Oracle, Microsoft, MuleSoft, Jitterbit, Workato, Snaplogic.

Также размывается граница между PaaS и IaaS. Эксперты все чаще относят к PaaS сервисы поддержки администраторов систем и баз данных.

Сервисы Database as a Service (dbPaaS) упрощают работу с СУБД и снижают стоимость владения ими. Gartner отмечает значительный рост сегмента dbPaaS, который становится лидирующим на рынке. Большинство современных компаний предпочитает потреблять базы данных в облаке по модели сервиса ввиду того, что самостоятельное развертывание и обслуживание баз данных – операция достаточно сложная и трудозатратная, особенно в компаниях, активно разрабатывающих ПО. В этом случае компании ожидают автоматизации таких операций, как создание конфигураций БД с высокой доступностью, кластеризацией, автоматическое резервное копирование и восстановление после сбоев, а также мониторинг.

Некоторые эксперты, например Ли Майлз из Red Hat, стали относить к PaaS защиту приложений и данных от сбоя системы или аварии на основной площадке размещения ИТ-системы через полное восстановление в облаке провайдера – Disaster Recovery as a Service (DRaaS). Как в любой облачной услуге, здесь применяется оплата по модели pay as you go, что значительно снижает расходы.

Много споров вызывает классификация Container as a Service (CaaS) – создание контейнеров и управление ими в облаке провайдера. Некоторые эксперты, в частности управляющий директор Selectel Максим Семенихин, относят его к PaaS, хотя большинство придерживаются мнения, что сервис занимает промежуточное положение ближе к IaaS.

Наиболее детально к структуре рынка PaaS подошла компания Gartner, насчитавшая на нем 21 сегмент (см. таблицу).

Название	Категория сервиса
abiPaaS (Cloud Analytics and Business Intelligence Services)	Аналитика и BI
apimPaaS (Cloud API Management Services)	Управление API
aPaaS (Cloud Application Platform as a Service)	Облачный сервис, обеспечивающий платформу для разработки и развертывания приложений в облаке
adPaaS (Cloud Application Development Services)	Разработка приложений
iPaaS (Cloud Enterprise Integration Platform Services)	Промышленная интеграционная платформа
mbPaaS (Cloud Mobile Back-End Platform Services)	Платформа разработки мобильных приложений
AI PaaS (Cloud Artificial Intelligence Platform as a Service)	Платформа для ИИ
bPaaS (Cloud Blockchain Platform Services)	Блокчейн-платформа
bpmPaaS (Cloud Business Process Management Services)	Управление бизнес-процессами
brPaaS (Cloud Business Rule Platform Services)	Управление решениями
cPaaS (Cloud Communications Platform Services)	Коммуникационная платформа
csPaaS (Cloud Content Services Platform as a Service)	Контент-платформа
dbPaaS (Cloud Database Platform Services)	База данных
dxpPaaS (Cloud Digital Experience Platform Services)	Платформа цифрового опыта
espPaaS (Cloud Event Stream Processing Services)	Обработка потока событий
fPaaS (Cloud Function Platform Services)	Платформа облачных функций
imdgPaaS (Cloud In-Memory Data Grid as a Service)	Распределенное хранилище объектов в памяти
IoT PaaS (Cloud Internet of Things Platform Services)	Платформа интернета вещей
mftPaaS (Cloud Managed File Transfer as a Service)	Управление переносом файлов
Cloud Master Data Management Services	Управление основными данными компании
Cloud Message Broker/Event Broker Services	Брокер сообщений
rpaPaaS (Cloud Robotic Process Automation Platform as a Service)	Платформа автоматизации бизнес-процессов

Источник: Gartner, Platform as a Service: Definition, Taxonomy and Vendor Landscape, 2019

По оценкам Gartner, сегодня на мировом рынке более 360 поставщиков предлагают свыше 550 сервисов PaaS. Ни один поставщик не охватывает все сегменты сразу, и 90% из них работают только в одном сегменте.

Российский рынок менее разнообразен. Эксперты iKS-Consulting выделяют на нем следующие категории сервисов:

- платформы для разработчиков, микросервисы (aPaaS, adPaaS, Kubernetes as a Service);
- виртуальный хостинг сайтов (веб-хостинг);
- платформы для обработки больших данных, аналитика (abiPaaS, Big Data as a Service);
- платформы для баз данных (DBaaS);
- платформы виртуальных АТС и видеоконференцсвязи;
- сети доставки контента (CDN);
- платформы для искусственного интеллекта, синтеза и распознавания речи и изображений (AI PaaS);
- M2M-платформы, в том числе платформы «умного» дома (IoT PaaS);
- App Containers (контейнеры приложений).

Пользователи PaaS

Сегодня компании, которые борются за эффективность и за клиента, все сильнее ощущают потребность в собственном ПО, которое позволит им внедрять собственные ноу-хау и отвечать на индивидуальные запросы клиентов. При

этом, как отмечает Владимир Карагиоз, руководитель группы архитекторов по решениям Red Hat, у бизнеса есть естественное желание не создавать такое ПО с нуля, а основываться на готовых программных компонентах с готовыми процессами разработки, тестирования и доставки софта. И в этом им приходят на помощь сервисы PaaS, решающие эти задачи.

Использование PaaS дает возможность приобрести отдельные готовые компоненты непосредственно у облачного провайдера, который поддерживает платформу, или у компаний, применяющих средства разработки, совместимые с соответствующей платформой. Это позволяет упростить и стандартизировать процесс разработки, а также минимизировать инвестиции на этапе запуска проекта, сократить время вывода облачного продукта на рынок и гибко подстраиваться под меняющиеся потребности рынка в дальнейшем. Облачные сервисы помогают внедрять пилоты и демонстрировать конечному заказчику преимущества предлагаемых решений.

Важный фактор роста популярности PaaS – широкое использование технологий контейнерной виртуализации, в частности переход на Kubernetes. Эта технология позволяет разработчикам, не обладающим глубокими знаниями системного администрирования, разворачивать сложные высокодоступные и отказоустойчивые топологии в облаке практически без при-

▲
Сегменты
рынка PaaS



Дмитрий Юдин, директор по развитию бизнеса технологий и облачных решений, Oracle в России и СНГ

Большая часть сервисов PaaS все еще предлагается иностранными облачными провайдерами. В России рынок PaaS растет, хоть и медленнее, чем в среднем по миру. При этом размер его пока существенно меньше, чем рынков SaaS и IaaS. По экспертным оценкам, объем рынка PaaS в России может составить в следующем году около \$100 млн.

включения системных администраторов. Спрос на PaaS-сервисы растет, так как они заменяют дорогую и немасштабируемую консалтинговую экспертизу извне, считает Илья Летунов, руководитель Mail.ru Cloud Solutions.

Среди достоинств PaaS для пользователей можно выделить следующие:

- отсутствие необходимости самостоятельно создавать и конфигурировать виртуальные машины – пользователю достаточно портала или скриптов для настройки баз данных;
- отсутствие необходимости разбираться в низкоуровневой детализации PaaS-решения;
- провайдер PaaS автоматически обновляет используемое программное обеспечение и СУБД, снимая эту задачу с пользователя, плата за лицензии взимается в рамках сервиса;
- задачи масштабирования и обеспечения высокой доступности сервиса входят в зону ответственности провайдера.

В России к сервисам PaaS прибегают в основном крупные и средние предприятия. Так, по оценке iKS-Consulting, их совокупная доля на рынке составляет 73% (рис. 1). Оставшиеся 27% делят практически в равных долях малые предприятия и корпорации.

С распространением облачных средств быстрой разработки ПО можно ожидать большего проникновения услуг PaaS в корпоративный сектор. Не исключен также рост интереса со стороны микропредприятий, хотя пока процент их в структуре пользователей услуг PaaS мал и не достигает 3%.

В отличие от IaaS и SaaS, торговля среди пользователей PaaS лишь на третьем месте: лидерство здесь за банками и ИТ-компаниями. Доля же сегментов «Транспорт и логистика», «Образование, инжиниринг, наука, медиа, реклама», «Госсектор», «Строительство», «Медицина и фармацевтика» и «Промышленное производство» в совокупности едва достигает 3%.

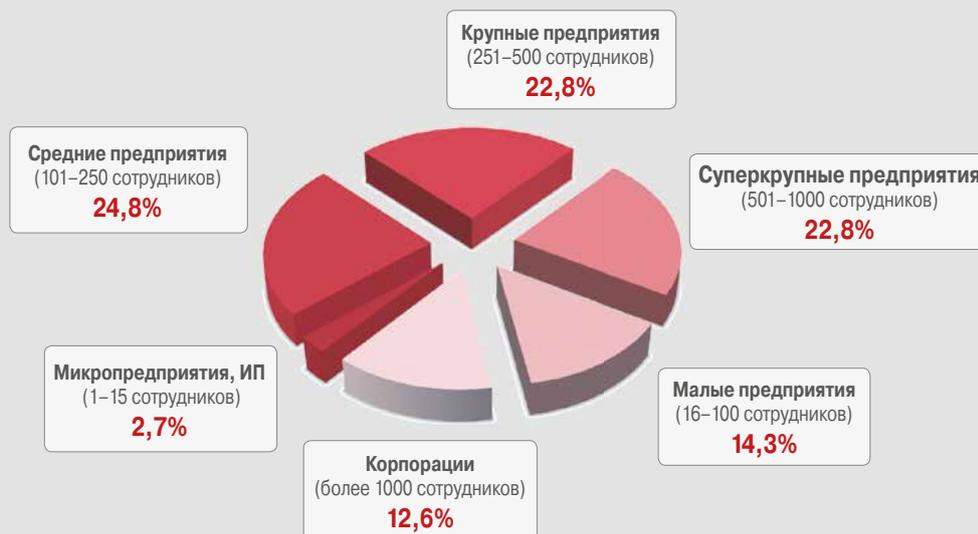
В региональной структуре пользователей услуг PaaS ожидаемо лидируют Москва и Московская область, занимая 55% рынка. Доли Санкт-Петербурга и Ленинградской области вместе немного превышают 11%. Вплотную за ними следуют Центральный (за вычетом Москвы и области), Южный и Дальневосточный федеральные округа с равными долями – по 8% рынка. А вот иностранных пользователей у услуг PaaS практически нет: выручка сегмента «Вне территории РФ» близка к нулю.

Поставщики PaaS

Наиболее популярными зарубежными PaaS-решениями в настоящий момент можно считать AWS Elastic, Google App Engine, Microsoft Azure (Azure Websites и Azure Cloud Services), Heroku, IBM Bluemix, Red Hat OpenShift и Jelastic. PaaS-сервисы управления данными предлагает Oracle.

Одной из первых крупных российских компаний, обративших внимание на PaaS, была «Яндекс», которая еще в 2012 г. разработала и запустила Cocaine – PaaS-систему с открытым исход-

Рис. 1. ▶ Структура пользователей PaaS в публичных облаках по размеру компании, 2017 г.



Источник: iKS-Consulting

ным кодом, аналог Google App Engine и Heroku, которую использует для внутренних разработок. Платформа поддерживает популярные языки программирования: C++, Java, Python, Ruby, Node.js, Go. В числе преимуществ Coscaine – наличие фреймворков, возможность приложений общаться между собой не только через http (это, например, позволяет построить свою платформу облачных вычислений), сильная поддержка изоляции приложений.

В последнее время и другие облачные провайдеры в поисках конкурентных преимуществ начали обращать внимание на предоставление по сервисной модели облачных платформ, причем и в публичных облаках.

Знаковым для российского рынка PaaS стал 2018 г. – провайдеры начали предлагать сервисы, связанные с контейнерной виртуализацией. Такие сервисы появились в публичных облаках Mail.ru, «Яндекса» и китайской Huawei, развернувших свои облака в ЦОДах Москвы и ЦФО. Эти компании активно конкурируют за целевую аудиторию с PaaS-провайдерами, предоставляющими свои сервисы из-за рубежа. Блокировки Роскомнадзора и российское законодательство способствовали перераспределению долей рынка в пользу локальных игроков.

Mail.ru предложила PaaS-сервисы на open source-решениях, развернутых на облачной платформе OpenStack. Большое внимание привлек запуск компанией проекта Kubernetes as a Service (KaaS), который значительно упрощает задачу разработчиков систем с микросервисной архитектурой.

Активно переносит свои PaaS-сервисы на территорию России Huawei. Нашим разработчикам стали доступны dbPaaS-сервисы: предоставление реляционных баз данных для MySQL, PostgreSQL, Microsoft SQL Server, баз данных, со-

Наша задача – вывести свои сервисы PaaS на уровень, при котором любой появившийся сервис мы могли бы интегрировать в облачную платформу Tiонix и предоставить клиенту, чтобы он не тратил время на его развертывание и поддержку.



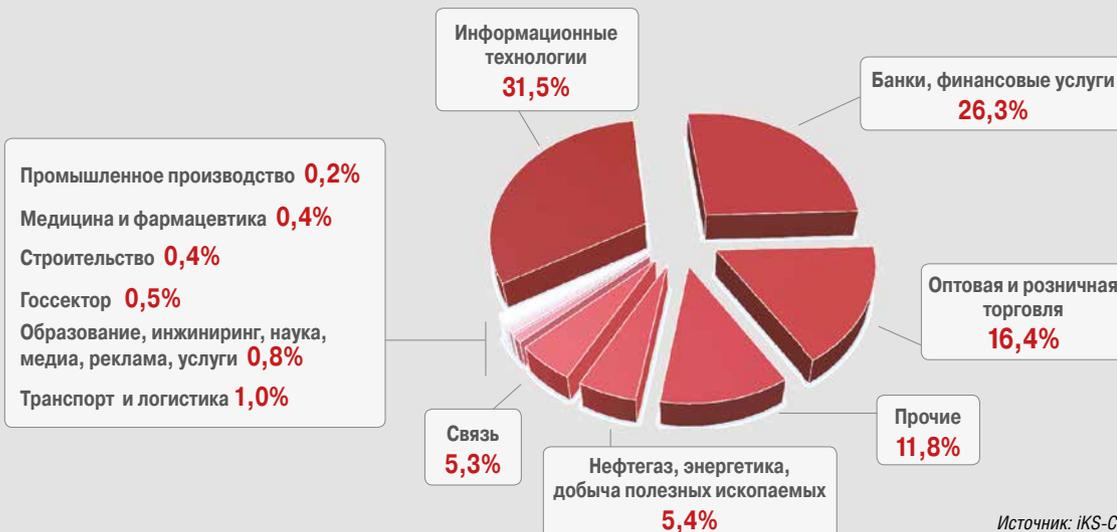
Антон Петров,
генеральный директор,
«Тионикс»

вместимых с MongoDB, а также сервисы распределенного кэша (imdgPaaS) для Redis и для Memcached.

Компания DataLine предлагает установить в своем облаке CloudLine на платформе VMware кластер Kubernetes и оптимизировать его под задачи заказчика. Компания обеспечивает обновление версий Kubernetes, управление инцидентами, поддержку актуальности сертификатов, организацию резервного копирования кластера и пользовательских данных. Другие PaaS-решения, предлагаемые компанией из своего облака: «1С как сервис» и «DevOps как сервис» – сопровождение всего DevOps-цикла: от обучения, внедрения DevOps-практик до готовой инфраструктуры Kubernetes с необходимыми CI/CD-инструментами. Выручка DataLine от услуг PaaS с 2017-го по 2018 гг. увеличилась на 25%.

Kubernetes as a Service вывел на рынок и «Ростелеком». Сервис развернут на национальной облачной платформе RTCLOUD. Входящая в ГК «Ростелеком» компания «Тионикс» реализовала мониторинг, бэкап и аналитику на интегрированных в платформу «Тионикс VDC» на базе OpenStack open source-решениях ELK, Zabbix, Vareos и Ansible и работает над коробочным решением.

Возможность быстрого создания кластера Kubernetes появилась и в виртуальном приват-



◀ **Рис. 2.**
Отраслевая структура коммерческих пользователей PaaS в 2017 г. (доли в выручке)

Источник: IKS-Consulting



Илья Летунов,
руководитель,
Mail.ru
Cloud Solutions

Фактически многие компании хотят получить полноценные озера данных под ключ, однако узким местом здесь является отсутствие культуры работы с данными. При этом Big Data PaaS как раз является катализатором изменений, предоставляя возможность создания полноценных песочниц для обработки больших данных всего за несколько часов, а не месяцев. Это позволяет компаниям строить и проверять гипотезы гораздо быстрее и формировать культуру работы с данными.

ном облаке Selectel: для этого в панели управления достаточно указать требуемые характеристики и количество нод.

Компания «Онланта» (ГК ЛАНИТ) предлагает «БИТ.Телефония как сервис» – платформу виртуальной облачной АТС, видеоконференцсвязь для бизнеса VideoMost. Среди других PaaS-сервисов – конструктор сайтов, резервное копирование в облако (BaaS) и объектное хранилище ONLANTA S3.

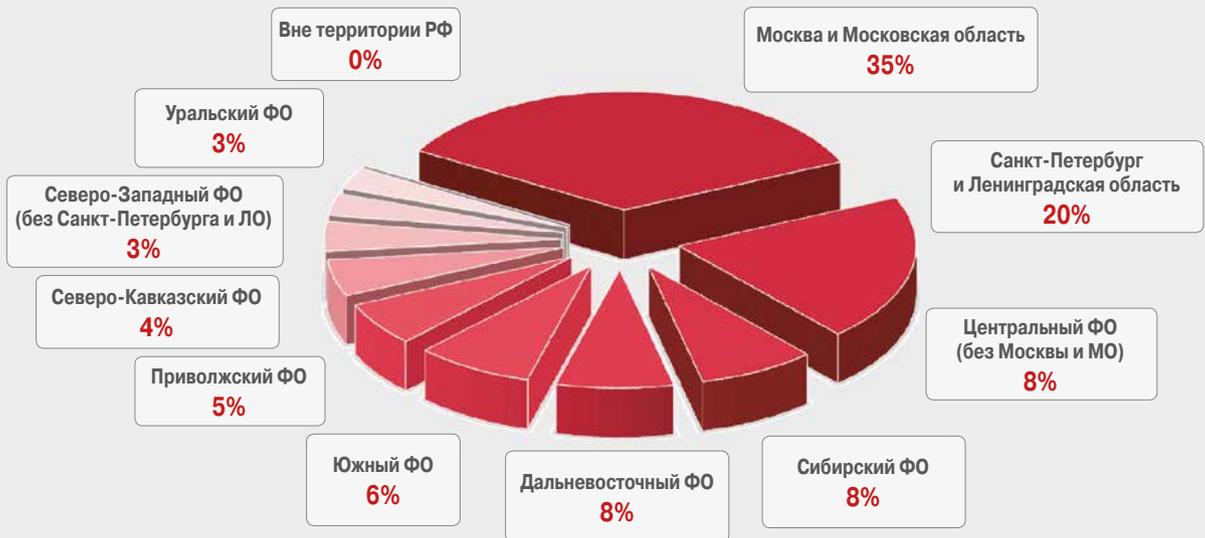
жет служить Kubernetes as a Service в публичных облаках компаний Mail.ru, DataLine и «Ростелекома».

Нельзя не отметить растущий спрос на огромный пласт сервисов для аналитики данных и машинного обучения. Так, Mail.ru зафиксировала потребность своих клиентов в PaaS для больших данных (Big Data PaaS). Компаниям уже недостаточно простой инфраструктуры для работы с большими данными, им нужны тесно интегрированные платформы для построения процессов их извлечения, распределенной обработки и хранения и организации самих хранилищ данных.

Наряду с классическими источниками больших данных (ритейл, FMCG) их генератором все чаще становятся IoT-устройства. Бурный рост рынка IoT приводит как к росту BigData PaaS, так и к появлению специализированных PaaS для IoT. Технологии интернета вещей активно развиваются, поэтому спрос на облачные платформы IoT PaaS для разработки решений в этой области будет только увеличиваться.

Настоящий бум переживают решения на основе технологий искусственного интеллекта. Предложения AI PaaS в основном сосредоточены на обучении, обработке естественного язы-

Рис. 3. ▶
Региональная структура коммерческих пользователей PaaS, 2017 г. (доли в выручке)



Источник: iKS-Consulting

РaaS-тенденции

Одна из тенденций облачного рынка – переход к мультиоблаку, объединяющему облачные платформы разных провайдеров с целью гибкого выбора наилучших по функциональности решений и оптимизации расходов. Эта тенденция справедлива и для рынка PaaS. Клиенты все чаще ищут решения Multicloud PaaS, а инструменты MegaPaaS (комплексный PaaS) помогают управлять рынком облачных платформ.

Сохраняется тенденция к интеграции сервисов IaaS и PaaS. Примером на нашем рынке мо-

ка и компьютерном зрении. У нас в стране растет популярность ИИ-чат-ботов, которые существенно снижают нагрузку на персонал колл-центров. Примером могут служить чат-боты на платформе «Алиса» компании «Яндекс», которая предоставляет инструменты для распознавания голоса и анализа сообщений. Системы распознавания образов применяются для идентификации преступников, номеров машин. Для поддержки разработчиков нужны облачные платформы, и не удивительно, что AI PaaS используются все шире. **ИКС**

Лучше меньше, да лучше



Тенденция развития электронной торговли – переход от e-commerce-сайтов и интернет-магазинов к электронным торговым площадкам и прайс-агрегаторам – наблюдается и в облачных сервисах. Причем разнообразие предложений у лидеров рынка SaaS-маркетплейсов увеличивается, а у других российских игроков – сокращается.

Николай Носов

«Многие компании на рынке SaaS уменьшили число предложений, поскольку попробовали и поняли, что это не их бизнес», – прокомментировал изменения на рынке Станислав Мирин, ведущий консультант консалтингового агентства iKS-Consulting, которое провело осенью этого года исследование рынка SaaS-маркетплейсов.

В то же время ведущие игроки укрепили позиции, расширив набор услуг на своих площадках. В полтора раза за год увеличила ассортимент решений из облака сохранив лидерство на рынке облачных маркетплейсов компания Softline, предоставляющая сервисы как российских, так и зарубежных поставщиков, в том числе в глобальных публичных облаках Microsoft Azure и Google Cloud Platform. Активно развивает маркетплейсы для своих клиентов банк Тинькофф. В отличие от других российских банков, называющих маркетплейсами

свои доски рекламных объявлений, Тинькофф имеет полноценные системы, позволяющие из личного кабинета выбрать и оплатить предлагаемые услуги. В тройку лидеров стремительно ворвалась компания Merlion, развернувшая маркетплейс на российской платформе электронной коммерции компании Velvica.

Что же такое маркетплейс?

Маркетплейс представляет собой оптимизированную онлайн-платформу для предоставления продуктов и услуг – электронную торговую площадку, на которой широкий круг поставщиков может арендовать «торговую точку» и предлагать покупателям свой товар. В случае облачных маркетплейсов – сервисы из облака.

В упомянутом исследовании iKS-Consulting маркетплейс определяется как решение агрегатора, на котором собраны сервисы различных

МНЕНИЕ ЭКСПЕРТА

Больше операций – больше затрат

Важнейшая задача дистрибьютора в цепочке поставок – снижение транзакционных издержек, возникающих при передаче продукта от производителя к потребителю. Каждая закупка и отгрузка требуют выполнения большого количества бизнес-операций, например документального оформления. Чем больше операций и чем меньше средний чек, что характерно для облачных маркетплейсов, тем больше затраты на организацию приема заказов, конфигурирования, выставления счетов, отслеживания

оплаты, дебиторской и кредиторской задолженности, поддержки партнеров и пользователей и т.д. Кроме того, потребители хотят иметь широкий выбор, так что число облачных услуг в маркетплейсах постоянно растет. Без сквозной автоматизации на базе бизнес-операционной платформы (BSS в терминах телекома) обслуживать такой поток становится невыгодно, а иногда и просто невозможно. Собственно, поэтому облачные дистрибьюторы развивают маркетплейсы и занимаются их сквозной автоматизацией на базе BSS-платформ.



Михаил Козлов,
эксперт РССПА



Антон Салов,
руководитель
проекта
MerliOnCloud

Выход на экономическую эффективность при реализации модели агрегации маркетплейсов происходит через четыре-пять лет. Отдачу получают те, кто раньше вложится и продолжит развивать бизнес.

поставщиков с возможностью моментального приобретения и управления всеми услугами из единого места. Таким образом, в число маркетплейсов аналитики не включают монобрендовые интернет-магазины (например, каталог услуг для бизнеса из облака Сбербанка) и витрины услуг, не обеспечивающие биллинга, – такие площадки скорее можно отнести к рекламным, работающим по другой бизнес-модели. Биллинговые системы нет смысла использовать при редких продажах крупных облачных услуг, скажем, услуг разработки проектных решений, – такие поставки проще отследить в CRM и обрабатывать вручную.

В число сервисов, продаваемых через SaaS-маркетплейсы, аналитики iKS-Consulting включают как услуги аренды программного обеспечения в облаке, так и покупку в облаке права на использование ПО на площадке заказчика. Подход понятный, поскольку современное ПО, как правило, имеет облачную составляющую: например, популярные у клиентов антивирусные средства неэффективны без использования постоянно обновляющейся облачной базы данных.

Бизнес-модели поставки облачных услуг

В классической схеме поставки облачных услуг SaaS-провайдер платит провайдеру IaaS-услуг за пользование облачной платформой и за аренду виртуальных вычислительных мощностей. В бизнес-модели SaaS-маркетплейса продажа конечному клиенту идет через реселлера – держателя маркетплейса, предоставляющего витрину разным SaaS-провайдерам. Маркетплейс привлекателен для конечного клиента за счет широкого спектра облачных услуг, возможности сравнения условий, цен и самостоятельного выбора сервисов.

Использующие маркетплейсы провайдеры облачных услуг расширяют рынок сбыта своих продуктов, опираясь на маркетинговые возможности реселлера, удобную и привычную для пользователей среду покупки.

Крупные SaaS-провайдеры сами создают свои магазины приложений – в 2018 г., по оценке некоторых экспертов, их имели 70% из 20 крупнейших по рыночной капитализации SaaS-компаний. Одной из первых торговых площа-

док SaaS была AppExchange компании Salesforce, запущенная еще в 2005 г.

Предоставление торговых точек сторонним разработчикам на своих площадках позволяет крупным компаниям укрепить позиции на рынке за счет расширения спектра предложений для конечного пользователя сервисов, не тратя ресурсов на их разработку. Это не только улучшает узнаваемость бренда, но и приносит ощутимую прибыль. Например, AppExchange приносит Salesforce \$2 млрд в год, причем доход от платформы в первом квартале 2019 г. составил 21% дохода компании и рос быстрее (36%), чем доход от продуктов Salesforce (16%).

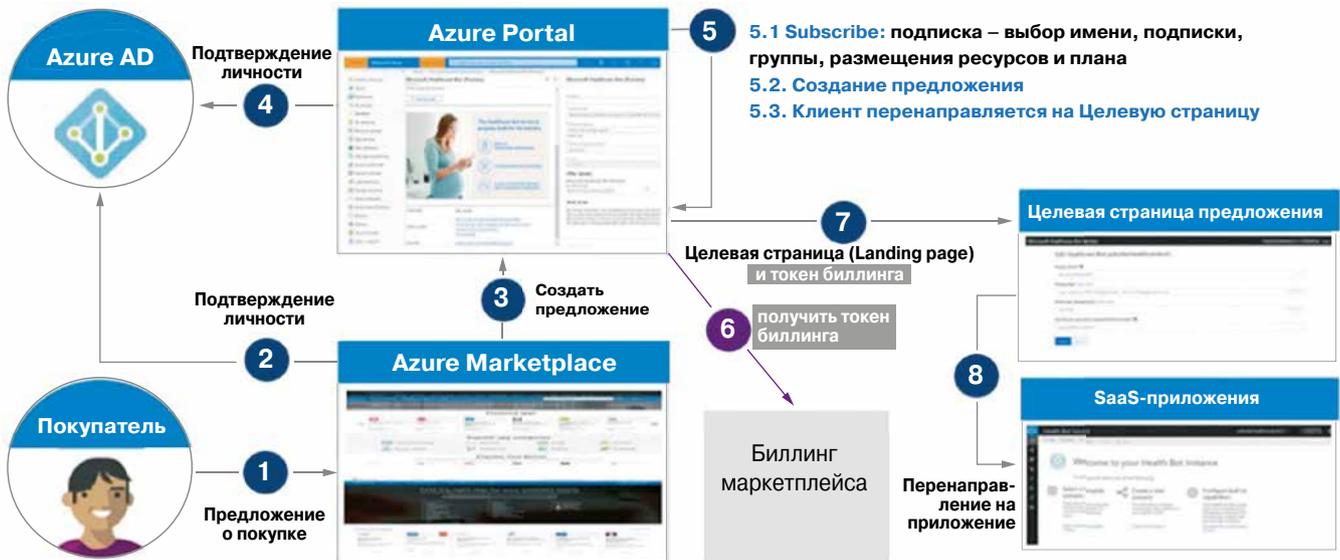
Партнерский маркетплейс

По оценкам BetterCloud, к 2022 г. 73% организаций планируют полностью перейти к потреблению приложений по модели SaaS. Число организаций, где 80% бизнес-приложений работает в облаке, к 2022 г. достигнет 86%. К таким прогнозам можно относиться по-разному, но в любом случае стоит отметить, что спрос на SaaS будет расти. Будет расширяться и номенклатура предлагаемых сервисов. Пользователю становится труднее выбрать оптимальное решение, которое ему нужно будет интегрировать с другими своими сервисами и в дальнейшем сопровождать. Если раньше сборку решения выполнял интегратор, что обычно дорого и долго, то теперь с просьбой собрать для него систему заказчик обращается к продавцу. При этом ему не нужна полная кастомизация, он хочет получить решение из готовых «кубиков», которые выбирает сам. В такой схеме часть функций интегратора переходит к реселлеру, который должен иметь экспертизу по продаваемым услугам, уметь собирать из готовых сервисов интегрированное решение и обеспечить его поддержку.

На облачном рынке набирают популярность партнерские программы. Например, программа Microsoft CSP позволяет заказчикам приобретать онлайн-сервисы Microsoft через провайдеров, причем за прошлый год такие продажи выросли на 40%. Провайдеры лучше знают локальный рынок, особенности национального законодательства, имеют удобные для бизнеса схемы оплаты.

Во многом на этом и основан бизнес российских облачных маркетплейсов, агрегирующих предложения гиперскейлеров и SaaS-провайдеров, которые предоставляют интересные для их клиентов сервисы. Если клиентами являются компании, сами предлагающие маркетплейсы для своих нишевых клиентов, то появляется еще одно звено – дистрибьютор для партнеров.

По такому пути пошла компания Merlion, создавшая платформу дистрибуции облачных сер-



Источник: Microsoft

висов. «Мы берем облачные решения вендоров и интегрируем их в нашу платформу, помогая канальным партнерам создать полноценные магазины с облачными сервисами. Маркетплейс Merlion – это не просто интернет-магазин облачных услуг, а мастер-каталог, из которого с нашей помощью партнеры создают свои витрины. Кроме того, мы предоставляем маркетинговую поддержку и услуги технического центра, в котором сертифицированные специалисты Merlion помогают внедрять облачные решения», – поясняет руководитель проекта MerliOnCloud Антон Салов. В настоящее время с направлением облачной дистрибуции Merlion сотрудничает 21 вендор. Среди них ведущие российские облачные компании «Яндекс», Mail.ru и глобальные игроки, такие как IBM. Повышенным спросом у клиентов пользуются решения в сфере безопасности. В ближайших планах Merlion – предложение рабочего места госслужащего из облака по сервисной модели.

Перспективы маркетплейсов

На глобальном рынке облаков сегодня быстрее всего растут облачные маркетплейсы гиперскейлеров, таких как AWS, IBM, Microsoft, Google и Alibaba, которые предоставляют разработчикам SaaS-решений интегрированные IaaS- и PaaS-среды. Наличие единой интегрированной платформы, как отмечает эксперт РССРА Михаил Козлов, позволяет относительно быстро переносить в облако традиционные приложения и/или разрабатывать новые cloud native-решения, которые лучше масштабируются при работе в распределенных облачных средах за счет применения микросервисной архитектуры и лучшей интеграции с базовыми сервисами платформы гиперскейлера. В итоге получается интегриро-

ванное SaaS-решение на базе глобальной платформы гиперскейлера, что решает многие проблемы разработчиков и их клиентов.

Примером может служить Azure Marketplace, предлагающий внешним партнерам свои площадки и системы авторизации (см. рисунок). Требование к партнерам, желающим разместить на этом маркетплейсе свои решения, – наличие лендинга (landing page), возможность интеграции приложения с Azure Active Directory и с API биллинговой системы маркетплейса.

Движение в направлении интегрированных платформ есть и на российском рынке. Активно развивает партнерскую программу на нашем рынке компания Huawei, которая уже размещает на своей инфраструктуре облачные сервисы сторонних вендоров, например сервис Cloud Gaming компании Loudplay. В российских реалиях в качестве таких гиперскейлеров могут выступить «Яндекс» и Mail.ru. Из последних новостей – запуск «Мегафоном» и Mail.ru «Платформы для бизнеса», совместного облачного сервиса, ориентированного на сектор SMB. Но пока это скорее интернет-магазины IaaS- и PaaS-услуг компаний, до полноценных облачных кросс-брендовых маркетплейсов российских гиперскейлеров, включающих портфель SaaS-услуг, дело не дошло. Будет ли развиваться такая модель продаж в России – покажет время.

Интеграция с платформой гиперскейлера может оказаться и недостатком. Многие заказчики хотят размещать SaaS-решения на своих платформах, да и зависимость от гиперскейлера нравится далеко не всем, особенно если это зарубежный гиперскейлер, поддерживающий санкции. Так что и для обычных маркетплейсов найдется своя ниша на российском рынке. ИКС

▲ Схема обработки запроса в Azure Marketplace

Сценарии использования облачной «песочницы»



Сергей Зинкевич,
продакт-менеджер,
«КРОК
Облачные сервисы»

Рост популярности облаков во многом обусловлен преимуществами, которые они обеспечивают при разработке, тестировании и «выводе в свет» новых ИТ-продуктов. Каковы основные сценарии работы с облачными «песочницами»?

Пять лет назад ключевыми клиентами облака КРОК были банки, ритейлеры, реже промышленники. Сейчас их начали теснить разработчики ИТ-продуктов. За последний год этот сегмент прирос на 15%. Мы стали разбираться, в чем причина повышенного спроса на облако среди этой целевой аудитории. Поверхностный анализ показал, что такие заказчики используют публичные облака для разработки и тестирования новых продуктов и клиентских сервисов. Профит связан с экономией и быстрым выводом на рынок, которые достигаются именно в виртуальной среде, а не на локальном физическом «железе».

Использование облаков для процессов разработки и тестирования (test/dev) сегодня распространено среди компаний самого разного масштаба. Их подключают и нишевые ИТ-разработчики, и крупные корпоративные клиенты. У последних в облаке, помимо продуктивных систем, «крутятся» тестовые среды для мобильных и веб-приложений. Данная тенденция наблюдается во всем мире. Существует даже мнение, что именно из-за повышения скорости разработки увеличивается популярность облачных сервисов. В 2018 г. впервые за все время, что IDC исследует мировой ИТ-рынок, расходы облачных провайдеров на свои инфраструктуры превысили траты на решения on-premise.

Работа с облачной «песочницей» – специальной средой для разработки, тестирования и «вывода в свет» нового продукта – происходит по нескольким сценариям.

1 Проверка гипотез и новых ИТ-продуктов

Это актуальная задача для команд владельца продукта, директоров по цифровой трансформации или ИТ-директоров, которые курируют вопросы развития цифровых сервисов. Часто для запуска новых сервисов необходимо привлечь внешних разработчиков ИТ-продуктов. Какой именно подойдет для конкретной компании, без предварительной проверки сказать сложно. Продуктов на рынке множество, проверить хочется каждый, но ИТ-руководители сталкиваются с естественными ограничениями. Не хватает ресурсов на развертывание тестовых сред: либо мощность инфраструктуры не позволяет, либо все руки в департаменте заняты. К тому же закупка нового оборудования – процесс небыстрый, связанный с долгими бюрократическими процедурами, из-за чего приобретать новые системы для тестовых нужд для ИТ-директора очень трудозатратно. Выход из ситуации – использование «песочницы», в которой можно одновременно запустить сколь угодно большое количество продуктов и проверить любые гипотезы достаточно быстро без утверждения дополнительного бюджета на покупку «железа» у финансового директора.

2 Разработка и тестирование как таковые

Не удивительно, что основной процесс, связанный с выводом продукта или услуги на рынок, часто переносят в облака. Среди преиму-

ществ «песочницы» – гибкая, быстро масштабируемая инфраструктура, благодаря которой можно подключать все новые и новые ресурсы. Особенно это актуально при нагрузочном тестировании, когда нужно воспроизвести среду, близкую к «боевым» условиям. Запуск аналогичного процесса в локальной инфраструктуре грозит перебоями в работе бизнес-систем, для которых может не хватить мощности.

Сегодня практически никто из крупных компаний не покупает оборудование специально под процессы test/dev, так как это нерентабельно. Тестирование – это периодически возникающие задачи с достаточно коротким циклом, поэтому облако подходит идеально. Дополнительный плюс облаков – прозрачная тарификация, позволяющая экономить деньги. Система биллинга с гранулярностью в один час позволяет рассчитывать затраты не только на тестирование в целом, но и по отдельным продуктовым командам и командам разработчиков.

3 Работа с непроверенными поставщиками или продуктами

В крупных компаниях, особенно финансовых, достаточно остро стоит вопрос подключения к инфраструктуре новых подрядчиков. В нашей практике есть проект, который хорошо это иллюстрирует. Банк, размещаясь в ЦОДе КРОК, решил внедрить инновационное решение от стороннего разработчика. Но из-за комплаенса и особых требований служб безопасности банка доступ нового подрядчика в периметр банка не утвердили. Чтобы решить проблему, мы предложили использовать облако КРОК. Вскоре система начала работать в доверенной среде, а заказчику не пришлось столкнуться с бюрократическими проверками со стороны внутренних подразделений банка.

4 Обучение и обмен опытом

Создание нового продукта и тестирование его функциональности – это всегда коллективная работа. Облако с его возможностью работать через консоль без привязки к стационарному месту особенно ценится среди разработчиков. Для крупных ИТ-компаний, у которых по всему миру могут быть сотни сотрудников, облако – это также способ оптимизировать затраты на управление проектными командами и обеспечить слаженность их работы. Кроме того, к системам, размещенным в облаке, достаточно просто предоставить доступ извне, чем пользуются компании при обучении своего персонала. Классический пример – компания Positive Technologies, которая в облаке не только развивает десять своих коммерческих продуктов, но и проводит обучение работе с программными средствами 60 российских и международных партнеров. **IKS**

Отчет дает углубленное представление о состоянии всего 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 оптимального сценария его развития. Отчет дополнен информацией об облачных провайдерах и партнерских альянсах, а также другими данными и выводами, дающими широкое и углубленное представление обо всем рынке.

Структура отчета «Российский рынок коммерческих дата-центров 2018–2023»

Введение	
Цель исследования	
Методика проведения исследования	
1. Текущее состояние рынка кЦОДов в России и в мире	1.1 Динамика развития в в 2018–2019 гг. <ul style="list-style-type: none"> • Основные показатели развития • Прирост совокупной емкости • Прогноз числа коммерческих стоек • Введенные емкости • Динамика сертификации российских кЦОДов • Структура доходов кЦОДов • Структура затрат кЦОДов 1.2. Динамика и прогноз развития мирового рынка 1.3. Структура рынка по основным сегментам услуг
2. Структура рынка	2.1. Отраслевая структура 2.2. Региональная структура 2.3. Структура по направлениям услуг
3. Лидеры рынка кЦОДов	3.1. Рейтинг по числу стоек 3.2. Рейтинг по доходам в сегментах Colocation / Cloud / Telecom
4. Региональные сегменты рынка коммерческих дата-центров	4.1. Москва и Московская область 4.2. Санкт-Петербург и Ленинградская область 4.3. Региональные кЦОДы 4.4. География и связность кЦОДов
5. Тенденции развития рынка дата-центров в 2018–2019 гг.	5.1. Изменения в бизнес-моделях кЦОДов 5.2. Облачные услуги в бизнесе кЦОДов 5.3. Масштабирование: мега- и микроЦОДы 5.4. Edge Computing: периферийные кЦОДы 5.5. Актуальны ли майнеры для ЦОДов 5.6. Услуги удаленного мониторинга инженерного и ИТ-оборудования
6. Конкурентная ситуация	6.1. Партнерские альянсы 6.2. Операторские и ведомственные дата-центры на рынке кЦОДов
7. Прогноз и перспективы развития рынка кЦОДов в 2019–2023 гг.	7.1. Факторы развития рынка кЦОДов в России 7.2. Прогноз динамики развития российского рынка кЦОДов до 2023 г. 7.3. Государство как заказчик услуг кЦОДов 7.4. кЦОДы и госпрограмма «Цифровая экономика» 7.5. Экспортный потенциал российских дата-центров
Приложение 1. Международная и российская сертификация	
Приложение 2. Интервью с руководителями ведущих коммерческих ЦОДов	
Приложение 3. Потребительские предпочтения на рынке кЦОДов	

ЗАО «IKS-холдинг»

www.iks-consulting.ru

Параметры отчета

- Стоимость: 159 000 руб. (без НДС)
- Объем отчета: более 100 страниц
- Количество иллюстраций: более 50
- Дата выхода: 12 сентября 2019

Подробная информация и заказ отчета

- Дмитрий Жаров
- E-mail: iks@iksmedia.ru
- Тел.: +7 (495) 150-6424 доб. 138

Игры в облаках



Николай Носов

Все более широкое распространение высокоскоростного интернета, увеличение потребления игр по сервисной модели и цифровая трансформация в индустрии медиа и развлечений – факторы, стимулирующие рост рынка IaaS.

Рынки и тенденции

«Что наша жизнь? Игра!», – пел Герман в опере «Пиковая дама». Утверждение, во многом ставшее известным благодаря заставке «Что? Где? Когда?», не является сильным преувеличением – люди много времени отдают играм. Игра – школа жизни и помощник развития в детстве, отдых и возможность отключиться от забот повседневности для взрослых, основа индустрии развлечений для бизнеса.

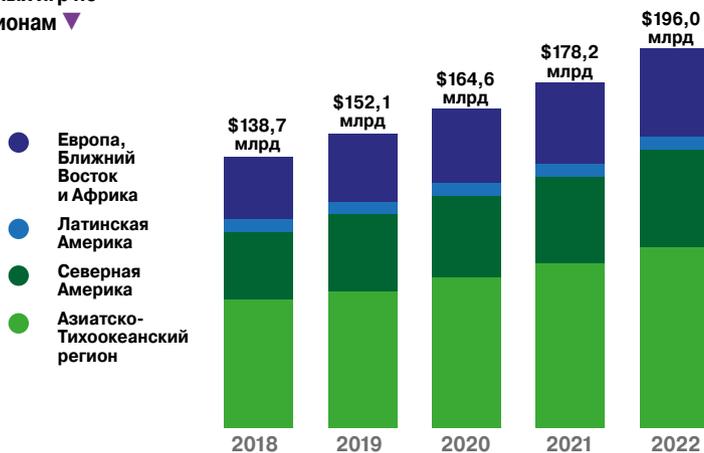
Новое время – новые песни. Игры стали цифровыми, не надо ходить в тренажерный зал или на стадион – достаточно включить компьютер и войти в интернет.

Индустрия компьютерных игр уже зарабатывает денег больше, чем индустрии кино и музыки вместе взятые, и отрыв продолжает увеличиваться. По оценкам NewZoo, в 2018 г. объем мирового рынка компьютерных игр достиг \$138,7 млрд и, прирастая ежегодно на 9%, достигнет в 2022 г. до отметки \$196 млрд (рис. 1). Впечатляет и объем российского рынка, который в 2019 г. составит \$1,88 млрд.

Одним из самых быстрорастущих (CAGR = 11,3%) является сегмент мобильных игр (со смартфонов и планшетов в совокупности), который уже в 2019 г. принесет доход в размере \$68,5 млрд (45% рынка). Выпуски новых консолей Xbox и PlayStation подстегнут рынок консольных игр, ежегодный рост которого оценивается в 13,4%. Сегмент игр, устанавливаемых на ПК, будет увеличиваться медленнее. Объем этого сегмента достигнет в 2019 г. \$32,2 млрд (21%), но его доля будет сокращаться (рис. 2).

Одна из ярко выраженных тенденций в развитии игровой индустрии – переход к централизо-

Рис. 1. Рост мирового рынка компьютерных игр по регионам ▼



Источник: NewZoo, Games Global Market Report 2019

ваным системам с переносом вычислений в дата-центр. В конце прошлого века были широко распространены однопользовательские игры – например, первые версии шутеров Doom или такие стратегии, как Command and Conquer. Следующим шагом стали массовые многопользовательские онлайн-игры, вроде World of Warcraft или Lineage. Текущий этап – облачные игры (cloud gaming).

Взрослые – большие дети. Им нравятся новые игрушки, а старые надоедают и отправляются пылиться на антресоли. Избавляющие от необходимости покупок новых физических предметов облака решают эту проблему. Поиграл – надоело – бросил. И можно запускать новую игру.

Сама идея использования облаков для игр не нова и в различных исполнениях существует более десяти лет. Из облаков можно загружать новые игры, обновлять их версии. В облаке, не привязанном к конкретному устройству, удобно хранить учетные записи пользователей и текущие результаты прохождения игр, организовывать взаимодействие находящихся в разных частях света игроков. Привязка к облачной платформе Google Maps позволила разработавшей мобильную игру Pokemon Go компании Niantic Labs установить рекорд – заработать более \$1 млрд за семь месяцев после запуска игры в августе 2016 г., причем в первый месяц только в США в нее играли более 10 млн человек.

В cloud gaming используется тот же подход, что и в сервисах стриминга музыки, – не нужно ничего скачивать, в один клик вы получаете желаемую музыку на любом устройстве, а доступная база композиций постоянно пополняется новыми альбомами. По такой же схеме стали распространяться компьютерные игры.

В 2018 г. с играми, которыми можно пользоваться без загрузки, начали экспериментировать социальные сети. Первопроходцем стала Facebook, запустившая в 2018 г. Instant Game. За самой популярной соцсетью последовала Google, а затем и соцсети азиатских стран: Tencent в Китае, Kakao в Южной Корее и LINE в Японии.

В октябре 2018 г. Microsoft анонсировала опирающийся на технологию cloud gaming проект Project xCloud. Активна компания Sony, чья облачная игровая платформа PlayStation Now имеет более 700 тыс. пользователей.

В марте 2019 г. Google анонсировала стриминговый сервис для геймеров Stadia, который позволяет запускать игры на любых устройствах, работающих с Google Chrome: компьютерах, смартфонах, планшетах и даже на телевизорах. Предполагается, что на момент запуска Stadia будет поддерживать разрешение 4K при кадровой частоте 60 кадров в секунду с HDR. В

Общая тенденция развития игровой индустрии – увеличение объема используемых вычислительных ресурсов в облаках, эластичность которых позволяет справиться с резкими перепадами нагрузки. Нагрузка возрастает вечером, когда люди приходят с работы, меняется и в цикле жизни игры: при запуске игры в результате рекламной кампании интерес максимальный, затем число пользователей уменьшается. Издателям игр нет смысла покупать для них оборудование – целесообразнее использовать модель IaaS, получать ресурсы по подписке или по факту потребления.

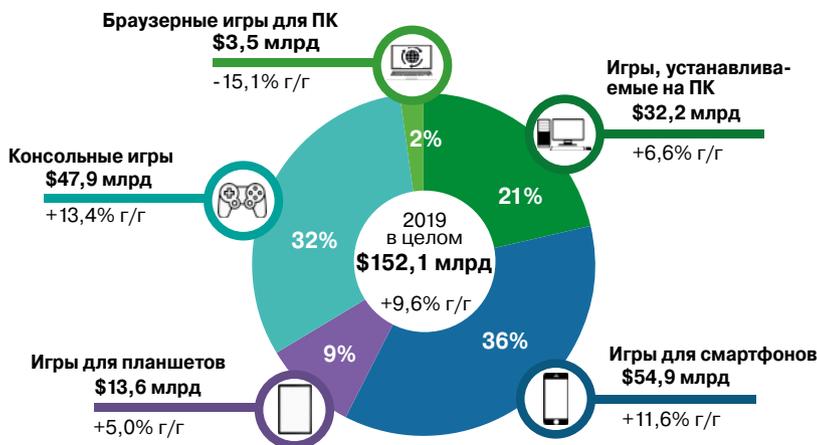


Илья Матвеев,
директор по развитию бизнеса, G-Core Labs

будущем компания планирует добавить поддержку 8K при 120 кадрах в секунду, причем джойстик можно будет подключать прямо к телевизору. В следующем году Google представит для коммерческого использования более 4 тыс. игр, которые будут распространяться по подписке стоимостью предположительно порядка \$15 в месяц.

Размещение контента игры в облаке сглаживает остроту проблемы хранения, увеличивает доступность и охват аудитории. Кроме того, облако помогает адаптировать игровой контент для разных пользовательских устройств. Облачные игры предоставляют пользователям ряд преимуществ, таких как высокая скорость, автоматическое обновление и масштабируемость. Ожидается, что ежегодный темп роста мирового

Рис. 2.
Сегментация мирового рынка компьютерных игр по типу используемых устройств ▼



Источник: NewZoo, Games Global Market Report 2019

го рынка облачных игр составит 24,69%, а его объем в 2023 г. достигнет \$3,8 млрд (рис. 3).

Участники рынка

К участникам рынка компьютерных игр можно отнести их производителей, пользователей и поставщиков услуг, обеспечивающих пользователям доступ к контенту.

Ключевые фигуры мирового рынка электронных игр – Sony Corporation (Япония), Game Fly, Nvidia Corporation, Ubitus, Playkey, Microsoft, Zynga, Cirrascale Corporation, Google (все США), PlayGiga (Испания), Tsinghua Tongfang (Китай) и Hatch Entertainment (Финляндия). Они разрабатывают периферийные устройства для игр, используют свою инфраструктуру или выступают пользователями для провайдеров IaaS-сервисов.

Люди играют в игры по-разному: одни сами гоняют мяч во дворе, другие смотрят соревнования по телевизору, третьи – скандируют кричалки на стадионах и сопровождают любимую команду на выездных встречах. Так и с компьютерными играми.

Компания NewZoo в своем отчете Games Global Market Report 2019 выделила восемь групп игроков.

Самые активные, Ultimate Gamers (13% пользователей), пользуются всеми видами игр. Их можно сравнить с футбольными фанатами, которые живут игрой своей команды и сами играют на любительском уровне.

All-Round Enthusiasts (9%) – также заядлые геймеры, играющие по многу часов в неделю. Но это не такие фанаты, как Ultimate Gamers. Как правило, это работники, занятые полный рабочий день, поэтому покупка новейших продуктов и оборудования не составляет для них проблемы.

Conventional Players (4%) – это обычные игроки, похожие на Ultimate Gamers 10 лет назад, до появления игрового видеоконтента и стремительного роста киберспорта. Смотреть, как игра-

ют другие, им неинтересно, но сами они играют и представляют интерес с точки зрения продаж современного оборудования для игр.

Time Fillers (27%) – это потребители, которые играют в игры, как правило, на мобильных устройствах во время поездок на работу и обратно. Есть свободное время, которое надо занять, – поиграли, но игры не являются важнейшей частью их жизни. Они редко проводят за игрой более нескольких часов в неделю.

Popcorn Gamers (13%) – любители смотреть трансляции игр и киберспортивных турниров. У них пользуются популярностью YouTube и специализирующийся на тематике компьютерных игр видеостриминговый сервис Twitch.

Backseat Viewers (6%) смотрят игровой или киберспортивный видеоконтент, но редко играют в игры. В основном это постаревшие геймеры, которым когда-то нравилось играть, но которые из-за работы или семейных обязательств больше не успевают это делать.

Hardware Enthusiasts (9%) – энтузиасты оборудования. Эти потребители не любят игры, играют не много, но просто не могут закрывать глаза на новейшие игры, используемые ими компьютеры и периферийные устройства, поэтому тратят большие средства на эти продукты.

Самая интересная для облачного рынка категория игроков – Cloud Gamers (19%), те, кто любят качественные игры, но не хотят тратиться на дорогостоящее оборудование. К ним относятся пользователи игровых облачных платформ Microsoft (xCloud) и Google (Stadia).

Облачные игровые компьютеры и 5G

При использовании технологии cloud gaming вычисления происходят не на локальном компьютере, а в дата-центре – видео на компьютер пользователя передается в виде потока. При такой схеме работы возрастает нагрузка на дата-центр – требуются высокопроизводительные компьютеры, мощные серверные графические процессоры и каналы связи. Важным фактором становится высокая скорость обработки и передачи данных. Приемлемая задержка не превышает нескольких миллисекунд, чтобы пользователь не успел заметить задержки между нажатием клавиши на клавиатуре и реакцией на экране.

Для продажи игр в нашей стране российским и международным компаниям понадобятся ЦОДы с хорошим временем доступа до конечного пользователя. И тут на отечественном рын-

Рис. 3. Прогноз роста мирового рынка облачных игр ▼



Источник: Market Research Future, Cloud Gaming Market Research Report – Global Forecast till 2023

ке преимущества получают российские дата-центры, расположенные в непосредственной близости от основной массы игроков.

Например, для того чтобы быть ближе к пользователю, компания G-Core Labs размещает вычислительные мощности по модели colocation в десяти российских дата-центрах в разных уголках России. В них развернуты облака, созданные на платформе OpenStack, а компания предлагает услуги игровому бизнесу по модели IaaS. Одна только компания Wargaming задействует для своих игр более 5 тыс. серверов G-Core Labs по всему миру. IaaS-сервис компании для доставки российским игрокам 250 игр использует компания PlayKey. Применяемая в облачном сервисе Playkey технология NVIDIA GRID vGaming позволяет одновременно запускать до 160 ПК-игр и транслировать мобильные игры для еще большего числа одновременных пользователей с помощью контейнерной технологии.

Среди других онлайн-сервисов цифрового распространения компьютерных игр и программ можно отметить Steam, разработанный и поддерживаемый компанией Valve.

Перспективным выглядит использование высокоскоростной беспроводной связи 5G и небольших edge-ЦОДов, обеспечивающих ее поддержку. В августе 2019 г. в Москве прошел первый в истории киберспортивный турнир, в котором задействовались технологии 5G и cloud gaming. Технологии 5G обеспечила компания Huawei, связь – компания «Мегафон», а за облака отвечала российская компания Loudplay. При работе через сеть 5G исчезают периодические существенные задержки, наблюдаемые в сетях 4G и критичные для динамических игр и киберспорта. Другой вариант применения 5G – игры в виртуальной реальности. Таких игр в силу отсутствия общепринятых стандартов на новую технологию на рынке пока нет, но они наверняка появятся в ближайшем будущем.

Технология cloud gaming помогает решить основную проблему пользователей – быстрое устаревание их компьютеров, которые просто не могут поддерживать работу современных игр.

Так, компания Loudplay делает виртуальный игровой компьютер для пользователя и сдает в аренду. На этом компьютере уже есть предустановленные игры, кроме того, пользователь может запустить на нем свои. По сути, компания на своей платформе предоставляет им удаленное рабочее место, аналогичное тому, что предоставляет Citrix, но оборудованное для игр.

Loudplay задействует облако Huawei в ЦОДах IXcellerate и 3data, причем китайская компания привезла в Россию и установила «железо» специально с учетом требований Loudplay. Также

Мы используем модель pay-as-you-go. Клиент вносит предоплату, а затем расходует средства на время, проведенное за игрой. Во взаимоотношениях с провайдерами мы прорабатываем модель revenue sharing – мы не будем платить за инфраструктуру, но провайдер заберет часть денег, вносимых игроками.



Виталий Стародубов, основатель и владелец, Loudplay

Loudplay работает с CDNvideo, облачными платформами «СБКлауд» и «СберКлауд». Перспективными для провайдеров облачных игр выглядят операторские ЦОДы, например облако #CloudMTC, так как у них помимо инфраструктуры можно воспользоваться каналами привлечения клиентов.

Сколько потребуется IaaS-провайдеров?

В нашей стране около 40 млн уникальных игроков, играющих в компьютерные игры ежемесячно. Доля устаревшего оборудования у них, по оценке основателя и владельца компании Loudplay Виталия Стародубова, превышает 80%. Из этих 40 млн только 15% безболезненно для бюджета смогут приобрести современный компьютер. Есть еще «спящие» игроки – как правило, возрастные, имеющие хороший доход. Им тоже будет интересен игровой компьютер из облака.

Если, по оценкам NewZoo, 19% игроков уже использует сервис облачного гейминга, то со временем их доля возрастет. В. Стародубов предполагает, что половина целевой аудитории будет готова воспользоваться сервисом облачного гейминга при среднем чеке 500 руб. в месяц. В этом случае потенциальный рынок российских облачных игр составит более 80 млрд руб., или почти \$1,3 млрд в год.

Если перевести эти цифры в объем необходимой инфраструктуры, то получится 51–85 тыс. серверов (при 14 млн игроков и выделении сервера на восемь игроков и загрузке 3–5%, создаваемой обычно игроками), или, как подсчитали в iKS-Consulting, 2500–4000 стоек.

Все эти выкладки сделаны для рынка B2C, но есть еще рынок обучающих игр для B2B, которые начинают все чаще применяться и тоже внесут свой вклад. Рынок облачных игр уже оказывает сильное влияние на отечественный рынок дата-центров, и его рост надо учитывать при прогнозировании нагрузки на ЦОДы. [IKS](#)

Мой ЦОД – моя крепость

Рубежи физической
безопасности дата-центра

Антон Котов, руководитель отдела,
«Инсистемс» (ГК ЛАНИТ)

ЦОД – это и несколько комнат в офисном здании, и несколько зданий с десятками машинных залов на территории в полсотни гектаров. Для обеспечения физической безопасности столь разных объектов нужны, разумеется, разные решения, учитывающие сценарии их использования.



Кратко описанные ниже технологии, сложившиеся отраслевые правила и стандарты относятся к ЦОДу, вновь возводимому на обособленной территории, – пожалуй, простейшему случаю с точки зрения проектировщика и строителя.

Главные моменты

Основные принципы, которые надо всегда держать в голове при проектировании и строительстве систем безопасности ЦОДа, на мой взгляд, очевидны. Главная цель работы – обеспечить сохранность и неприкосновенность носителей информации, вычислительного оборудования и оборудования передачи данных.

Защита должна быть многослойной – несколько рубежей безопасности, преодоление которых усложняется от периферии к центру. Важно обеспечить максимальный контроль передвижений и действий посетителей вплоть до сопровождения со строгостью конвоя. Влияние персонала на принятие решения о допуске на объект необходимо ограничить так, чтобы на территории ЦОДа не было мест, куда один человек через очередной рубеж безопасности может кого-либо пропустить одной условной кнопкой. Работу персонала нужно постоянно контролировать с помощью видеорегистрации, анализа передвижений и действий по логам системы безопасности.

Дальний кордон

Некоторые эксперты работу по обеспечению безопасности предлагают начинать с выбора места для строительства ЦОДа – подальше от дорог и неблагоприятных районов. На практике определяющими факторами становятся доступность и стоимость энергоресурсов и линий связи на площадке, а значимость критерия безопасности на этом этапе невелика. Конечно, по соседству с пиратской Тортугой или ненасытной Ордой безопасность ЦОДа обеспечить будет непросто, но профессионалы справятся.

Итак, есть участок, где будет построен ЦОД. Первый рубеж, который можно и нужно проектировать и строить, – внешнее ограждение. Шедеры заборостроения вдоль Рублево-Успенского шоссе позволяют говорить, что в этой области отечественная промышленность является одним из мировых лидеров, и задача специалиста по безопасности – воспользоваться этим лидерством наиболее полно. Строгий минимум высоты ограды – 2,5 м, ниже нельзя, иначе забор перестает быть сколько-нибудь серьезной преградой для злоумышленников. Забор углубляем на 50–70 см, чтобы затруднить возможный подкоп, а сверху украшаем «егазой», чтобы перелезть было невозможно. Растительности внутри и снаружи на расстоянии не менее 1 м быть не

должно – так мы обеспечим возможность наблюдения и снизим риск ложных срабатываний датчиков.

Современный забор немислим без видеонаблюдения, поэтому камеры должны быть установлены через каждые 30 м, а на поворотах и спусках/подъемах еще чаще. Длина фокуса объектива видеокамер на периметре – предмет расчетов и тестов, секторы обзора камер должны пересекаться. Детекция движения обязательна, трекинг объектов весьма желателен. В дополнение к камерам предусматриваем охранные извещатели, лучевые или, например, вибрационные. Да, возле забора обеспечиваем освещенность около 50 лк – это для патрульных сотрудников службы безопасности (видеокамеры должны видеть и в темноте). Разумеется, все перечисленные технические средства должны взаимодействовать: по сигналу тревоги от охранного извещателя включается освещение (на участке тревоги в темное время суток), изображение от ближайшей камеры выводится на оперативный монитор поста охраны, ближайшая поворотная камера на территории автоматически наводится на участок тревоги, то же происходит и по детекции движения в кадре видеокамер. Пожалуй, теперь за первый рубеж можно быть более или менее спокойным.

Кого-то все-таки придется впустить

Забор не может быть сплошным, нужно устроить проход и проезды. Хорошая практика – обустройство двух КПП, отдельно для входа/въезда и для выхода/выезда. Кроме того, должны быть пожарные ворота, которые будут открываться только для проезда пожарных.

Входной (въездной) КПП неплохо было бы организовать прямо в здании ЦОДа или в административном здании. На входе всё как обычно: интроскоп для багажа, рамка металлоискателя, ручной сканер у охранника. Детекторы радиации, взрывчатых веществ и опасных жидкостей – опционально. Для персонала обязателен алкотестер (с запретом прохода при положи-



тельном результате теста), для посетителей он желателен. Количество проходов, а значит, и остального оборудования зависит от размера ЦОДа и модели его использования (в корпоративном хранилище данных вряд ли стоит ожидать существенного трафика, а в дата-центре, предоставляющем услуги colocation, бывает весьма оживленно, особенно первое время).

Получение пропуска посетителем (и забывшим пропуск сотрудником) желательно максимально автоматизировать. Участие персонала КПП в этом процессе должно быть сведено к минимуму. Автоматизированный киоск, терминал, выдающий пропуск при предъявлении паспорта, – актуальное решение, но и «ручной» вариант тоже работоспособен. Разумеется, предварительно должна подаваться заявка, иметься система согласования этой заявки (обязательно более одной согласующей инстанции). Видеокамеры должны детально фиксировать все дей-

На въезде: болларды, шлагбаумы, площадка для досмотра. Видеокамеры снимают спереди, сзади, а также общий план. Отдельная камера необходима для распознавания регистрационного номера, съемка днища – опционально. Движение постороннего транспорта по территории ЦОДа должно быть ограничено: только от КПП до логистической площадки для погрузки/разгрузки и на выезд. Исключение может быть сделано только для автомобилей экстренных служб, топливозаправщиков с топливом для дизель-генераторных установок и самих ДГУ на базе автомобилей и прицепов. Стоянка любого автотранспорта, кроме технологического (погрузчиков, уборочной техники, гольф-каров для персонала и пр.), на территории ЦОДа должна быть запрещена, все паркуются за забором.

Выходящие из ЦОДа должны пройти через рамку металлоискателя. Сумки, рюкзаки и прочая ручная кладь досматриваются через интро-



ствия персонала КПП при выдаче пропуска.

Необходимо контролировать пронос на территорию средств вычислительной техники и носителей информации (включая флешки и даже гибкие магнитные диски) – их нужно указывать в заявке на пропуск

и согласовывать. Можно предусмотреть шкафчики для временного хранения вещей, запрещенных на территории ЦОДа.

Вход – через шлюзовую кабину, для всех. Проход снимается на видео и контролируется охранником. После прохода у посетителя должна быть возможность подойти только к стойке регистрации (выход на территорию и доступ в какие-либо помещения без сопровождения исключены).

скоп (кстати, правила авиакомпаний для ручной клади вполне применимы и в ЦОДах).

Автотранспорт, выезжающий из логистического центра ЦОДа, должен быть опломбирован. Номер пломбы, время пломбирования и ее соответствие транспортному средству должны быть переданы сотруднику КПП, выпускающему транспорт. На выезде – только внешний осмотр, видеосъемка регистрационного номера для распознавания автомобиля, съемка спереди, сзади, общим планом. Затем автоматизированная проверка пломб (задача охранника – только поднести сканер к пломбе), разрешение на выезд и подъем шлагбаума. На выездной дороге также не будут лишними болларды – вдруг кто-то попытается прорваться.

Приведенный список мероприятий для обеспечения безопасности на рубеже КПП не является исчерпывающим, можно его дополнять и



расширять, усложняя алгоритмы прохода и проезда. Или же все стоит упростить и облегчить. Здесь многое зависит от степени профессиональной деформации руководителя службы безопасности ЦОДа. Технически достижимо все.

Внутри дата-центра

Теперь нам нужно пустить сотрудников и посетителей в помещения ЦОДа в соответствии с их правами доступа, и это отнюдь не простая задача – десятки клиентских групп, сотни помещений! Одних только инженеров в дежурной смене может быть несколько десятков с разными уровнями и зонами доступа – к системам связи, электропитания, обеспечения микроклимата; вычислительные системы обслуживаются разными специалистами и в разных местах. А еще есть подрядчики (от клининга или доставки питьевой воды до специалистов службы поддержки производителей оборудования), есть и начальство.

В администрировании прохода помогает система контроля управления доступом. Часто именно ошибки администрирования приводят к нарушениям технологических регламентов: если специалист из-за того, что ему не предоставили доступ, вовремя не проверит установку или не заменит датчик с ошибочными показаниями (частый случай – пыльные дымовые пожарные извещатели), связисты не обеспечат соединение, то может произойти технический инцидент, в результате – скандал, финансовые и/или репутационные потери.

Базовый список средств обеспечения безопасности в здании (технологическом модуле) ЦОДа выглядит так:

- для помещений с невысоким уровнем безопасности (складов, кладовок для инвентаря и пр.) – дверь закрывается на ключ, охранная сигнализация на открывание двери;
- для технических помещений вспомогательного назначения (венткамер общеобменной вентиляции вспомогательных помещений, электрощитовых с «бытовыми» нагрузками) – контроль доступа или ключ, охранная сигнали-

зация на открывание двери, дверь должна просматриваться видеокамерой;

- для технических помещений обеспечения основных технологических процессов (помещений ИБП, электрощитовых с критически важными нагрузками, ГРЩ, щитовых для размещения оборудования диспетчеризации и автоматизации, коридоров, примыкающих к машинным залам и/или ведущих к ним и пр.) – контроль доступа на вход и выход, видеонаблюдение снаружи и внутри, охранная сигнализация на открывание двери и по объему помещения.

Для ключей обычно предусматриваются электронные ключницы, получение и сдача ключей – по идентификатору (карте), выход с объекта без сдачи ключа запрещается. Возможно снятие помещения с охраны при получении ключа от него.

В отдельную группу можно выделить помещения специального назначения: помещения для обработки информации, составляющей гостайну, помещения для хранения оружия (при наличии вооруженной охраны объекта). Правила и способы обеспечения безопасности таких помещений регламентируются нормативами, которые следует строго выполнять.

Последний рубеж

К машинным залам особое отношение, здесь самый высокий уровень безопасности, самые сложные алгоритмы прохода, самая изощренная техника. Обычно делаем так:

- на входе ставим шлюз, проход по одному, пройти в машзал можно только через него и больше никак;
- максимально усложняем алгоритм прохода – требуются два или три идентификатора с удаленным подтверждением доступа;
- обязательно применяем биометрические считыватели вместе с традиционными;
- организуем детальную видеофиксацию всего процесса прохода;



- устанавливаем охранную сигнализацию на пролом стен машзала;
- устанавливаем охранные извещатели между рядами стоек с возможностью индивидуального управления;
- монтируем видеокамеры между рядами стоек и в проходах так, чтобы секторы обзора пересекались, «мертвые» зоны исключаются.

В зависимости от сценария использования ЦОДа может потребоваться разделение машзалов на зоны клиентского доступа (разные арендаторы – разные задачи). Уровень безопасности в выделенных зонах необходимо будет обеспечить по запросу клиента, а также организовать внешнее управление видеонаблюдением и выдачу информации оператору клиента. Возможность предоставления такого сервиса должна быть заложена при проектировании, на неподготовленной площадке оперативно обеспечить такую услугу будет очень непросто и хлопотно.

Пары слов заслуживает организация видеонаблюдения в машзалах. Вообще, картинка с камер в машзалах получается довольно унылая: ряды темных шкафов с редкими проблесками индикаторов. Постоянно записывать это нет смысла, поэтому запись ведется только при движении/событиях, а в остальное время – не более четырех кадров в секунду. Кроме стационарных камер неплохим подспорьем в организации эффективного видеонаблюдения могут быть носимые видеорегистраторы у персонала и клиентов: устанавливать отдельную камеру у каждой стойки дорого, проконтролировать состав и качество выполняемых персоналом манипуляций «от первого лица» другим способом, как правило, нельзя. Выдачу и возврат регистраторов можно организовать по карте, после смены запись переносится в общий видеоархив. При желании можно обеспечить запрет на вход в машзал/зону машзала без видеорегистратора.

Есть еще один момент на стыке физической и информационной безопасности, требующий внимания, – пронос и применение в машзалах собственных электронных устройств представителей клиента. Если ноутбук, например, нужен для работы и без него обойтись нельзя, необходимо разрабатывать регламент, контролировать, проверять и перепроверять. Клиентам можно предоставлять необходимые устройства во временное пользование (правда, это не лучший вариант с точки зрения безопасности клиентской информации). Все личные устройства (смартфоны, планшеты и пр.) рекомендуется оставлять снаружи, ведь в них есть и фотоаппарат, и микрофон, и карта памяти. Конечно, решение этого вопроса – прерогатива специалистов по безопасности конкретного объекта, но при проектировании и строительстве несложно

предусмотреть камеру хранения (пару-тройку шкафчиков) и стационарный телефон для связи из машзала с внешним миром.

Невидимый рубеж

Выше перечислены, пожалуй, все основные технические решения для обеспечения физической безопасности ЦОДа. Но только ими не обойтись, нужен еще комплекс организационно-административных решений и мер – регламентов, постоянно обновляемых инструкций, а также жесткий контроль за их исполнением.

Упомянутый выше анализ логов действий операторов – один из инструментов безопасности. Анализируя и сравнивая действия операторов, можно выявить недостатки подготовки персонала (например, если какое-либо действие занимает у одного из операторов значительно больше времени, чем у других), недостатки в алгоритмах работы службы безопасности (многократные повторения допустимых действий без очевидных причин, повторные запросы на разрешение в течение короткого времени), предпосылки к сговору (многократное повторение совместных действий, разрешение на определенное действие, исходящее от одного и того же человека, регулярно дает один оператор). Для объектов с небольшим штатом актуальность, глубину и периодичность такого анализа может определить только владелец. Для больших ЦОДов систематический анализ обязателен, его автоматизация и внедрение должны быть предусмотрены при создании дата-центра.

Дальше будет легче?

Новые средства обеспечения безопасности появляются каждый день. Камеры становятся совершеннее, датчики точнее и «умнее». Участие человека в эксплуатации и защите ЦОДа уменьшается. Принципиально нового уровня безопасности можно достичь, на мой взгляд, с помощью роботизации, в идеале – создать этакий zero human data center. Да, это потребует принципиально новых подходов к проектированию, новых конструктивных решений для самих дата-центров, но результат может с лихвой покрыть издержки за счет снижения вероятности человеческих ошибок, основного источника проблем при эксплуатации ЦОДа.

Еще одна перспектива – автоматизированный анализ действий и передвижений персонала по видео, способный выявить необычные и подозрительные действия людей на территории дата-центра (пока на объекте есть люди, за ними надо присматривать). Подобные системы сегодня есть только у таких ИТ-гигантов, как Amazon, и они не затрагивают сегмент ЦОДов, но недолго осталось ждать внедрений и в дата-центрах. ИКС

Утечки трафика: можно ли починить фундамент Глобальной сети



Протокол BGP не накладывает никаких ограничений на то, что каждый оператор может делать с трафиком. И операторы в результате ошибки могут перенаправить на себя трафик магистральных каналов целых континентов и создать колоссальные проблемы для себя и других.

Артем Гавриченко,
технический директор,
Qrator Labs

У протокола динамической маршрутизации BGP (Border Gateway Protocol) юбилей: ему исполнилось 30 лет – согласитесь, солидный возраст для технологии. Но в повседневной жизни о BGP мало кто слышал, хотя все мы, не зная об этом, пользуемся протоколом каждый день. BGP – это невидимое и неосознаваемое нечто, связывающее множество разрозненных сетей разных стран и компаний в единый глобальный интернет на уровне маршрутизации. По сути он является краеугольным камнем архитектуры современной Глобальной сети.

Зачем о BGP нужно знать даже рядовому бизнес-пользователю? Дело в том, что любой бизнес, строя свои информационные системы, рано или поздно задумывается о создании собственной сети и, соответственно, вынужден формировать свою автономную систему (набор IP-сетей и маршрутизаторов, управляемых одним или несколькими операторами). И тогда он становится участником глобальной многоходовой игры под названием BGP. Но если правила в игре нарушаются, то происходят утечки трафика и злонамеренные его перехваты, а все из-за того, что «болезни» у протокола, несмотря на зрелость, остались теми же, что и у тинейджера.

Так, 25 ноября 2018 г. для пользователей «Ростелекома» оказались недоступными тысячи сервисов. Среди них были Amazon, YouTube, «ВКонтакте», онлайн-кинотеатр IVI и многие другие. Это был глобальный сбой в российском сегменте интернета, в результате которого пострадали более 5 тыс. операторов связи.

«Правда в том, что ложки нет»

Начнем с истории интернета. Самая важная вещь о нем, которую нужно знать: никакого интернета на самом деле нет.

Нет какого-то единого пространства как сущности, кому-то принадлежащей и кем-то управляемой. То, что мы называем интернетом, – это набор независимых и весьма разнообразных по своей природе сетей: не только сетей операторов связи, но и корпоративных систем, сетей доставки контента и многих других. Эти сети абсолютно самостоятельно принимают решение, с кем они хотят иметь отношения и на каких условиях.

Допустим, в 1985 г. сеть Alice Ltd подключилась к сети Bob & Co, а спустя 10 лет компания Bob & Co подписала договор о сотрудничестве с корпорацией Compaq Inc. Если в тот момент руководство компании Bob & Co разрешило фирмам Alice и Compaq обмениваться своими данными через сеть Bob & Co – вероятно, не бесплатно, – то с 1995 г. сеть Bob стала транзитной, а между IP-адресами сетей Alice и Compaq возникла связность. Множество таких, индивидуально принятых решений и формирует глобальную связность, которую мы привыкли называть интернетом.

Чтобы упростить подключение одной сети к другой, сети, участвующие в интернете, в основном используют один и тот же протокол – BGP – для обмена информацией о доступности IP-адресов и построения маршрутов. BGP позволяет обмениваться информацией о маршрутах движения трафика между автономными системами – независимыми сетями, которые составляют интернет.

Проблема в том, что BGP – протокол очень старый, он разрабатывался в конце 80-х годов. Тогда и вплоть до 1992 г. в интернете присутствовали в основном сети либо отдельных энтузиастов, либо крупных компаний, где работали достаточно квалифицированные сетевые инженеры. Авторы BGP не могли предвидеть, что в 1992 г. Тим Бернерс-Ли ошастливит весь свет, придумав «мировую паутину» World Wide Web (WWW) –



систему гипертекстовых веб-сайтов, из трафика которых сейчас по большей части и состоит интернет.

Преимущества WWW перед прежними способами обмена данных были очевидны. Всего за семь лет интернет прошел путь от заумной технологии для гиков до бума доткомов – компаний, достигших с помощью WWW миллиардной капитализации. Следствием такого сумасшедшего роста стал коллапс принятия решений. Если ранее любые изменения в Сети осуществлялись после общения небольшого числа квалифицированных специалистов и занимали около года, то в результате экспоненциального роста интернета принятие глобальных решений стало затягиваться на годы и десятилетия.

Хорошим примером служит протокол IPv6, идущий на смену старому протоколу IPv4. Его принято называть новым протоколом адресации, однако изобретен этот «новый» протокол был в 1996 г. Сегодня в числе внедряющих его инженеров и те, кто еще не родился, когда IPv6 начали вводить в эксплуатацию.

Что исправлять?

В далекие 80-е общее количество операторов связи исчислялось сотнями, протоколы и стандарты создавались на основе доверия специалистов друг другу, а все ошибки достаточно быстро исправлялись через личные знакомства. Поэтому в протоколе BGP не было прописано никаких ограничений относительно того, что каждый оператор может делать с трафиком.

BGP используется для того, чтобы сообщать «миру», к каким сетям можно получить доступ через данную автономную систему. Он не подразумевает никакой аутентификации и верификации полученных маршрутов к сетям. Так вот, ничто не мешает оператору в условном Бутово

объявить на весь мир, что он теперь является провайдером услуг связи для сетей Google и YouTube. Ввиду недостатков BGP сделать это можно случайно. И такие «случайности» происходят с завидной регулярностью.

Небольшие операторы в результате тривиальной ошибки могут перенаправить на себя трафик магистральных каналов передачи данных целых континентов. В результате они не только выведут из строя собственные сети, но и создадут колоссальные проблемы для других. Такие инциденты принято называть утечками маршрутов (route leaks).

Одним из самых значительных подобных инцидентов стала аномалия, созданная корпорацией Google. В результате ошибки конфигурации в сети Google перенаправила на себя трафик между японскими операторами и операторами в США. Вследствие этого на несколько часов доступ к большинству ресурсов в мире для пользователей в Японии оказался затруднен. Отличился и Китай, который уличили в систематическом перехвате интернет-трафика. Государственная телекоммуникационная компания China Telecom якобы на регулярной основе осуществляла перехват и перенаправление в Китай интернет-трафика, адресованного в США и Канаду или проходящего через эти страны.

В Зимбабве же в начале этого года случилось массовое отключение интернета на фоне обострения политической обстановки: блокировка локальных операторов довольно странным способом – через отключение их BGP-префиксов крупнейшими операторами на границе. Из-за этого анонсы страны не могли перейти вовне и оставались локальными, и трафик не мог найти дорогу «обратно» до пользователей.

Один из последних инцидентов произошел 6 июня текущего года, когда трафик швейцар-

ского дата-центра Safe Host, направленный в США, пошел «в обход» через China Telecom. В результате крупнейшие европейские сети (Swisscom, KPN, Bouygues Telecom, Numericable-SFR) были недоступны более двух часов.

Что делает оператор после того, как пропускает через себя трафик? Да все что угодно: он может записывать его, настраивать фишинговые сайты, искать в передаваемых данных пароли, финансовые и персональные данные. Для потенциального злоумышленника BGP становится идеальным инструментом для перехвата трафика и кражи данных.

Спасает пока лишь то, что еще не все кибервоины достаточно квалифицированы, чтобы понимать, что такое BGP и как с ним работать, но те, кто в курсе, давно используют недостатки протокола себе на пользу. Взять, например, спам. IP-адреса, с которых рассылается спам, довольно быстро оказываются в разнообразных черных списках, поэтому злоумышленникам эти адреса нужно оперативно менять, и здесь им на руку оказываются уязвимости BGP, позволяющие воровать чужие неиспользуемые IP-сети.

От угроз перехвата трафика не спасает даже шифрование. Благодаря ошибкам BGP можно практически для любого ресурса в интернете получить сертификат шифрования, абсолютно идентичный легитимному, и подписать им поддельный сайт. Далее с использованием этого сертификата можно перехватывать любые данные. Итог – колоссальные убытки для бизнеса, при том что пользователи в принципе не могут заметить подмену ресурса.

Не так давно в ходе атаки были похищены логины и пароли клиентов криптобиржи MyEtherWallet.com. Используя протокол BGP, злоумышленники смогли перенаправить трафик DNS-сервиса Amazon на свой хост и на несколько часов подменить выдачу записей DNS сайта MyEtherWallet.com на выдачу DNS подготовленного фишингового сайта, расположенного в России. В течение почти двух часов никто не замечал этой подмены, и люди вводили свои учетные данные на фальшивом сайте. В результате этой операции кто-то разбогател на 215 ETH (около \$140 тыс.).

Работа на годы вперед

Сейчас в мире насчитывается почти 60 тыс. операторов связи, при этом профессионализм их сетевых инженеров уже далеко не так высок, как раньше, да и взаимного доверия от специалистов с разных континентов вряд ли стоит ожидать.

Проблема с внедрением вышеупомянутого протокола IPv6 состоит в том, что для смены версии протокола IP необходимо перенастроить все устройства в мире, от смартфонов до борто-

вого компьютера МКС. С BGP в теории все проще – нужно лишь обновить сетевые устройства операторов, коих в мире на несколько порядков меньше. Однако операторы очень не любят что-либо обновлять, потому что любое изменение в сети может привести к отказу в обслуживании и перебою в связи, а бесперебойность связи – это по большому счету единственный KPI сетевых операторов.

Вот из-за этого разрыва между теорией и практикой и возникают проблемы, от которых мы все страдаем.

На протяжении десятилетий операторское сообщество пытается справиться с BGP-аномалиями. На этом пути уже было несколько вех. Одной из последних стала технология BGPsec – расширение протокола BGP, добавляющее пошаговые криптографические подписи для наиболее важных атрибутов BGP. Но BGPsec пока не получил широкого распространения, так как реализация криптографических алгоритмов – это тяжелая вычислительная задача, на которую нужно тратить серьезные ресурсы, а разнообразное дешевое оборудование, популярное у операторов, даже минимальное шифрование в «живой» сети не способно обеспечить.

Сейчас в профессиональном сообществе готовится новая, наиболее эффективная в краткосрочной перспективе, итерация решения этого вопроса под названием ASPA (Autonomous System Provider Authorization), в разработке которой принимает участие и Qrator Labs. Поскольку причиной большинства утечек является некорректная настройка протокола, единственным способом «лечения» становится устранение условий, при которых ошибки инженеров способны влиять на других операторов связи. Опциональные механизмы фильтрации нужно встроить в сам протокол, тем самым упростив и автоматизировав его настройку. По сути, будет создан «автопилот автомобиля Tesla» для BGP: водителя целиком это не заменит, но существенно облегчит жизнь и снизит аварийность.

Однако даже в случае полного успеха и принятия профессиональным сообществом этого подхода его реализация займет годы, поскольку нужно менять сам протокол: соответствующие изменения должны быть внедрены значительным числом операторов в мире или по крайней мере самыми крупными из них.

Вся история технологий и человечества в целом представляет собой постоянные циклы развития. Мы уверены, что к своему 40-летию BGP, как и интернет в целом, уж точно повзрослеет, станет более надежным, управляемым и безопасным протоколом. Мы приложим к этому максимум усилий. ИКС

Контейнерная виртуализация: преимущества и проблемы безопасности



Михаил Кондрашин, технический директор, Trend Micro в России и СНГ

Сегодня контейнеры массово используют для разработки и развертывания приложений, а само понятие стало таким же привычным, как «виртуальная машина», «облако» или «сервер». Но большой интерес к контейнерам проявляют и киберпреступники.

Хотя контейнеры и технологии контейнеризации известны достаточно давно, настоящую популярность они получили после появления в 2013 г. платформы Docker, связанного с ней активного сообщества пользователей и старта инициативы ОСИ (Open Container Initiative). Помимо ряда явных преимуществ, есть у контейнеров недостатки и уязвимости, которыми могут воспользоваться в своих целях киберпреступники. Поэтому разговор пойдет не только о самих контейнерах, но и о возможных путях их защиты от хакеров.

Преимущества контейнеров

Программисты любят контейнеры в первую очередь за гибкую среду, которая позволяет создавать их намного быстрее, чем те же виртуальные машины. Так же быстрее происходит их запуск и остановка. Помимо этого, контейнеры намного менее требовательны к ресурсам системы. Как правило, их «вес» измеряется не

гигабайтами, а мегабайтами, так как при контейнерной виртуализации нет нужды «упаковывать» всю ОС, чтобы приложение нормально функционировало. Вместо этого все контейнеры используют ядро системы хоста, высвобождая огромное количество ресурсов и позволяя установить намного больше таких контейнеров на один хост.

Несмотря на совместное использование ядра, все приложения изолированы друг от друга. Они не могут друг на друга влиять, даже если в каком-нибудь из них произойдет ошибка. Это значит, что разработчики свободно могут изменять параметры своих приложений и не опасаться, что их программа «положит» весь сервер. Эта же изолированность и использование ядра без нужды в гостевой ОС, как в виртуальных машинах (с которыми у контейнеров, кстати, немало общего), позволяют без проблем переносить контейнеры с приложениями с сервера на сервер. Помимо этого, применение контейнеров упрощает

управление версиями и обновление приложений, так как обновление софта в одном контейнере не повлияет на остальные части системы.

К другим преимуществам технологий контейнеризации стоит отнести активное сообщество. Из-за популярности этой темы практически любая проблема, с которой столкнулся разработчик, либо уже была решена кем-то еще и описана на форумах, либо быстро найдет свое решение. По той же причине в Сети хватает публичных библиотек-репозиториях с контейнерами, а над совершенствованием экосистемы контейнерной виртуализации и инструментами для разработки и управления ими трудится огромное количество специалистов со всего мира. Причем многие решения касаются автоматизации процессов, которые позволяют построить цепочки непрерывной интеграции, развертывания и доставки (Continuous Integration, Continuous Delivery/Deployment, CI/CD) практически без участия пользователей.

Недостатки контейнеров и угрозы безопасности

Среди основных недостатков контейнеров следует назвать повышенную сложность управления большим их числом в системе (которого легко достичь из-за малого «веса» самих контейнеров). Для решения этой задачи часто применяются дополнительные инструменты, например Kubernetes. Далее, в рамках одной системы можно использовать только контейнеры, построенные для конкретной архитектуры, например для ОС Windows, так как все они задействуют ядро самой системы, а не гостевые ОС, как в виртуальных машинах. При этом для ресурсоемких приложений будет эффективней использовать не контейнеры или те же виртуальные машины, а традиционный сервер с прямым доступом к его ресурсам.

К явным угрозам безопасности можно отнести публичные репозитории, которые помогают развивать технологии контейнеризации. В исследовании Cisco Talos выяснилось, что на портале Docker Hub уже три года контейнеры Alpine Linux распространялись с пустым паролем суперпользователя, а дальнейшие исследования Kenna Security подтвердили, что эта же проблема касается примерно 20% всех контейнеров на том же ресурсе. Кроме того, взлом публичного реестра образов и добавление злоумышленниками собственных библиотек позволяют заразить все серверы, в кэше которых хранится этот образ, поскольку по умолчанию серверы таких реестров являются доверенными ресурсами.

С уже упоминавшегося Docker Hub в июне 2018 г. было удалено 17 таких контейнеров, но количество их загрузок за это время перевалило

за 1 млн. Более того, в конце апреля 2019 г. репозиторий был взломан и в руки хакеров попали данные свыше 190 тыс. пользователей, что вызывает неослабевающий интерес злоумышленников к этой сфере. А в конце мая 2019 г. прошла очередная волна распространения контейнеров с криптомайнером, использующим API Docker. Осенью 2018 г. из каталога PyPi также были удалены зараженные контейнеры, причем вредоносный код в них мог даже подменять адреса Bitcoin-кошельков жертв на нужные хакерам.

Рекомендации по кибербезопасности

Современный непрерывный процесс разработки и развертывания приложений, т.е. тот самый CI/CD, явно нуждается в переходе от обеспечения безопасности «по факту» к внедрению инструментов безопасности в сам процесс разработки. По данным Gartner, в этом году уже более чем в 70% корпоративных процессов разработки будут внедряться инструменты для автоматизированной оценки уязвимостей и настроек различных компонентов и пакетов из внешних open source- и коммерческих источников.

Оптимальным решением в данном случае было бы использование не отдельных приложений и инструментов, а единого комплексного решения, программного комплекса, способного самостоятельно обнаруживать вредоносное ПО и библиотеки и выявлять уязвимости (включая уязвимости «нулевого дня»), предотвращать выполнение и развертывание контейнеров в случае, если они были скомпрометированы, и обеспечивать соответствие требованиям к кибербезопасности международных регуляторов, которые сейчас крайне серьезно относятся к защите данных пользователей.

В целом же для защиты контейнеров и процесса разработки приложений компаниям необходимо принять следующие меры:

- обеспечить проверку безопасности на всех стадиях разработки, от кодирования до контейнеризации приложения;
- максимально автоматизировать эту процедуру проверки;
- распределить уровни доступа к механизмам проверки безопасности в зависимости от конкретной роли каждого участника разработки;
- обеспечить поддержку Docker Registry V2 API для сканирования образов контейнеров в реестрах.

Только с принятием таких мер можно будет снизить количество выявленных атак и проблем с безопасностью, которые неизбежно появляются из-за интереса киберпреступников к любому новому и популярному инструменту для разработки ПО. **ИКС**

ИБП со встроенными модульными smart-батареями

Компания Schneider Electric представила расширение линейки Galaxy: ИБП Galaxy VS со встроенными модульными smart-батареями. Решение разработано для удовлетворения потребностей в бесперебойном питании ИТ-оборудования периферийных, малых и небольших центров обработки данных, а также для важных объектов инфраструктуры коммерческих и промышленных предприятий. Модели доступны в диапазоне мощности от 10 до 50 кВт (400 В) и поддерживают разные типы батарей: свинцово-кислотные и литий-ионные.

Встраиваемые в ИБП Galaxy VS батареи позволяют устройству работать в автономном режиме от 5 до 60 мин, делают решение компактным и подходящим для различных типов нагрузок: от ИТ-нагрузки удаленных филиалов до небольших



промышленных систем. Батареи-ные блоки выполнены в виде легкоъемных модулей отказоустойчивой архитектуры, что дает возможность сократить время восстановления и организовать внутреннее резервирование батарей по схеме N + 1.

Решения линейки Galaxy VS позволяют снизить операционные расходы за счет эффективности до 99% в режиме EConversion и до 97% в режиме двойного преобразования. Новые компактные ИБП линейки Galaxy VS занимают на 25% меньше места.

ИБП Galaxy VS готовы к интеграции в EcoStruxure и обладают сертификатом Green Premium, подтверждающим энергоэффективность предлагаемого решения.

www.schneider-electric.ru

Гигабитные настраиваемые PoE-коммутаторы



Компания D-Link выпустила PoE-коммутаторы DGS-1100-10MP/C, DGS-1100-26MP/C, DGS-1100-26MPP/C новой аппаратной версии. Устройства предназначены для применения в профессиональных системах IP-видеонаблюдения, видеоконференцсвязи, в беспроводных и локальных сетях государственных и коммерческих организаций, медицинских, социальных и образовательных учреждений, использующих PoE-совместимое оборудование с высоким уровнем энергопотребления.

Новая версия выполнена на платформе с увеличенной производительностью процессора и объемом памяти, поддерживает большой размер пакета Jumbo-фрейм, функционал PD Alive, отслеживающий доступность PoE-устройств с возможностью их перезапуска в случае сбоя питания. Для DGS-1100-26MPP/C максимальная мощность на PoE-порт (порты 21–24) увеличена до 90 Вт (IEEE 802.3bt).

Коммутатор DGS-1100-10MP/C оснащен восемью портами 10/100/1000Base-T с поддержкой 802.3af/802.3at PoE (30 Вт) и двумя портами 1000Base-X SFP, PoE-бюджет – 130 Вт.

DGS-1100-26MP/C оснащен 24 портами 10/100/1000Base-T с поддержкой PoE 802.3af/802.3at (30 Вт) и двумя комбо-портами 100/1000Base-T/SFP, PoE-бюджет – 370 Вт.

DGS-1100-26MPP/C оснащен 24 портами 10/100/1000Base-T и двумя комбо-портами 100/1000Base-T/SFP (порты 1–24 с поддержкой PoE 802.3af/802.3at (30 Вт), порты 21–24 с поддержкой 802.3bt (90 Вт)), PoE-бюджет – 518 Вт.

Модель DGS-1100-10MP/C выполнена в компактном металлическом 11-дюймовом корпусе, а DGS-1100-26MP/C и DGS-1100-26MPP/C – в 19-дюймовых корпусах.

Функционал безопасности коммутаторов включает D-Link Safeguard Engine, Traffic Segmentation, Broadcast/Multicast/Unicast Storm Control. Устройства поддерживают управление качеством обслуживания (802.1p QoS / DSCP), сети VLAN (802.1Q, Auto Surveillance VLAN, Voice VLAN), управление многоадресной рассылкой (IGMP Snooping, MLD Snooping) и повышение отказоустойчивости (Link Aggregation, Loopback Detection, 802.1D, 802.1w). Технология ERPS обеспечивает быстрое восстановление связи при отказе одной из линий в кольце. Мониторинг, просмотр и анализ статистики проходящего трафика реализован с помощью функции Port Mirroring.

www.dlink.ru

Роторный ИБП 2 МВт с литий-ионными батареями

Роторный ИБП UNIBLOCK UBT+2000, по данным его производителя компании Piller, – самый большой в мире ИБП единичной мощности, работающий как с традиционными свинцово-кислотными, так и с литий-ионными аккумуляторными батареями. Одна установка по своей мощности (2 МВт) эквивалентна системе из нескольких включенных параллельно модулей ИБП, построенной на базе других технологий.

Устройство обладает высокой масштабируемостью, позволяя устанавливать параллельно до 16 модулей по 2 МВт, что дает возможность создавать системы мощностью до 32 МВт. Кроме того, данная технология обеспечивает полный спектр вариантов проектирования системы – от обычных конфигураций на низком и среднем напряжении до решений IP-Bus, оптимизирующих эффективность и доступность системы электропитания и отвечающих уровням отказоустойчивости Tier III и даже Tier IV в конфигурации N + 1.



ИБП UNIBLOCK UBT+2000 характеризуется высокой энергоэффективностью – в режиме онлайн КПД составляет 97%. Капитальные затраты из расчета стоимости ИБП за 1 кВт значительно ниже, чем у решений меньшей единичной мощности, а расходы на эксплуатацию сведены к минимуму за счет отсутствия силовых конденсаторов и параллельного включения силовых модулей внутри ИБП. Как и современные серверы, которые защищает ИБП, установка способна работать при повышенных температурах, что в большинстве случаев исключает необходимость в применении систем кондиционирования воздуха.

www.piller.com

PDU с автоматическим переключением линии электропитания



Компания Tripp Lite создала специальное решение распределения питания (PDU ATS) на основе модели Tripp Lite PDUMH20HVAT.

Модель Tripp Lite PDUMH20HVAT оснащена измерителем тока с отображением информации на дисплее. Два входных кабеля обеспечивают возможность отдельного подключения к основному и резервному источникам питания. При нормальных условиях автоматический переключатель вводов поддерживает непрерывную подачу электропитания на все розетки от основного ввода. В случае неустойчивой работы основного ввода или его полного отказа функция автоматического переключения обеспечивает переключение на резервный ввод до момента восстановления устойчивой работы основного источника питания. Стандартное время проверки устойчивой работы ввода до возврата – 8 с, но по требованию заказчика оно может быть уменьшено до 1 с.

Tripp Lite PDUMH20HVAT имеет слот для карты SNMP для управления по сети.

www.tripplite.ru

Внутрирядный кондиционер с плавным регулированием производительности

Компания Conteg выпустила внутрирядный кондиционер CoolTeg Plus XC30 холодопроизводительностью до 22 кВт, который наилучшим образом подходит для дата-центров с тепловой нагрузкой до 100 кВт.

Кондиционер работает по принципу непосредственного охлаждения и оснащен двухроторным компрессором с бесщеточным двигателем постоянного тока (BLDC). Компрессор управляется инвертором постоянного тока, благодаря чему обеспечивается плавное регулирование производительности в диапазоне 10–100%. Компрессор, наряду с прочими компонентами, размещен во внутреннем блоке, который соединяется с выносным конденсатором при помощи трубопроводов хладагента. Такая конфигурация защищает все важные детали от неблагоприятных погодных условий (высокие и низкие температуры, дождь, снег, песчаные бури). Рабочий диапазон наружных температур составляет от –45 до +55°C. Хладагент – R410A.



Аппарат укомплектован электронным расширительным вентилем и современной системой управления, а также реле низкого и высокого давления. Отличается низким уровнем вибраций. Для удобства технического обслуживания предусмотрены запорные клапаны. Ширина внутреннего блока – 30 см. Длина трассы между внутренним и наружным блоком – до 60 м.

К внутреннему блоку CoolTeg Plus XC30 можно подключить любой наружный конденсатор с плавным регулированием скорости вращения вентиляторов. Размер и тип конденсатора определяют, исходя из условий на месте установки – в соответствии с температурой конденсации хладагента и наиболее часто встречающейся максимальной температурой в регионе. Для правильного подбора наружного блока следует использовать программу CoolTool или связаться с техническими специалистами Conteg.

www.conteg.ru

HOSSER TELECOM SOLUTIONS

Тел.: (812) 363-1193
Факс: (812) 363-1194
E-mail: spb@h-ts.ru
www.h-ts.ru с. 58–59

ITK

Тел.: (495) 542-2222
Факс: (495) 542-2224
E-mail: info@itk-group.ru
www.itk-group.ru с. 63

MARIOFF

Тел.:
(495) 933-1175
www.marioff.com/ru ... 1-я обл.

RITTAL

Тел.: (495) 775-0230
Факс: (495) 775-0239
E-mail: info@rittal.ru
www.rittal.ru с. 48–49, 57

SCHNEIDER ELECTRIC

Тел.: (495) 777-9990
Факс: (495) 777-9992
www.schneider-
electric.com с. 42–43

Указатель фирм и организаций

3data	11, 13, 83	Infinidat	6	Schneider Electric	6, 9, 11, 14, 15, 16, 37, 42, 43, 94	«Золоторудная компания Павлик»	21
451 Research	36	Infomatica	70	Schüco	29	«ИКС-Медиа»	4, 7, 10, 11, 36
Alibaba	5, 77	Integracia	7, 9	Selectel	11, 70, 73	«Импульс»	37
ALP Group	23	Intel	46	Servertech	39	«Инсистемс»	84
Alpha Software	70	ISTRADIGITAL	12	ServiceNow	70	«Иркутскэнерго-связь»	20
Amazon	5, 69, 88, 89, 91	ITCandor	45	Shaw Communications Facility	33	АО «КОНСИСТ-ОС»	12
AppGyver	70	IVI	89	Siemon	6, 62, 64	АНО «Координационный совет по ЦОДам и облачным технологиям»	12, 13
Appian	70	IXcellerate	4, 5, 11, 13, 83	Singapore Airlines	16	Корпорация развития Дальнего Востока	22
Apple	66	JAEGLI	58, 59	Snaplogic	70	КРОК	78, 79
ASHRAE	31, 59	JetBrains	66, 67	Softline	75	«КРОК Облачные сервисы»	78
Atos	9	Jitterbit	70	Sony Corporation	81, 82	«Лаборатория Касперского»	23
AWS	72, 77	John Deere	26	Stulz	38	ГК ЛАНИТ	74, 84
Betty Blocks	70	Kakao	81	Swisscom	59, 91	МВД	11
Bouygues Telecom	91	Kenna Security	93	Telehouse	52	«Мегафон»	77
C3 Solutions	9, 37	KPN	91	Tencent	81	Министерство РФ по развитию Дальнего Востока и Арктики	22
CABERO	28	Kuika	70	The Cerebrus Group	14	Министерство цифрового развития, связи и массовых коммуникаций РФ	4, 5, 11, 12, 22
CDNvideo	11	Lansa	70	Tosh Temir Savdo	8	Министерство юстиции РФ	12
Centron	29	ГК Legrand	39	Trend Micro	92	Минсельхоз России	26
China Telecom	5, 91	Lenovo	16	Trendfocus	45	Московская межгородная телефонная станция № 9	60
Cirrascale Corporation	82	LINE	81	Tripp Lite	9, 95	МТС	7, 20, 21, 22
Cisco	16, 43, 93	Linxdataloader	11, 60	Tsinghua Tongfang	82	МЧС	11
Citrix	6, 83	Logz.io	51	Ubitus	82	Наташкинский ГОК	19
Colobridge	50	LongJump	69	Valve	83	Находкинский завод минеральных удобрений	19
Conteg	95	Loudplay	77, 83	Vantiq	70	«Национальная химическая группа»	19
Credit Swiss	59	Magdeburg	59	Velvica	75	«Онланта»	74
Darktrace	53	Mail.ru	73, 74, 77	Vertiv	36, 37	«Полус»	19
DataLine	5, 13, 73, 74	Mail.ru Cloud Solutions	72, 74	VMware	16, 69, 73	«Порттелеком»	20
DataPro	11	Marioff	33	Workato	70	«Пульсар»	40
Dell	16, 43	Mendix	70	Xelent	11	РЖД	21
Dell Boomi	70	Merlion	75, 77	YouTube	89	«Росатом»	21
Dell EMC	44, 46, 47	Microsoft	5, 69, 70, 72, 73, 75, 76, 77, 81, 82	Zabbix	73	Росгвардия	11
DESY	59	Mordor Intelligence	44	Zuznow	70	«Росгеология»	21
D-Link	94	MuleSoft	70	Zynga	82	«Роснефть»	19, 20
Eaton	41	MyEtherWallet.com	91	Агентство Дальнего Востока по привлечению инвестиций и поддержке экспорта	22	«Ростелеком»	5, 20, 21, 73, 74, 89
EllInfor	46	NASA	69	Агентство по развитию человеческого капитала на Дальнем Востоке	22	«Ростелеком-ЦОД»	11
Equinix	59	NetApp	16, 44, 46, 47	«АйДи – Технологии управления»	65	«Росэнергоатом»	12
ERGO Research & Advisory	8, 9	NewZoo	80, 82, 83	Амурский газоперерабатывающий завод	19	ИНТЦ «Русский»	21
Facebook	81	Niantic Labs	81	«Балтийский лизинг»	11	«Радком»	20
Forrester	69	Nlyte	51	Билефельдский университет	29	Сбербанк	76
Forward Insights	45	Numericable-SFR	91	ВДНХ	30	СИБУР	19, 20
Future Facilities	51	NVIDIA	47, 82, 83	«Вертолеты России»	21	«Сколково»	25
Game Fly	82	Oracle	46, 54, 56, 70, 72	«Вконтакте»	89	Тинькофф	75
Gartner	14, 45, 47, 50, 69, 70, 71	Orange Business Services	20	«Восток»	21	«Тионикс»	73
G-Core Labs	81, 83	OrangeGrid	70	Восточный нефтехимический комплекс	19	«Транстелеком»	20
Google	5, 24, 52, 67, 69, 72, 75, 77, 81, 82, 90	OutSystems	70	Восточный центр государственного планирования	22	ТСХА	30
Grand View Research	45, 69	Pillar	39, 40, 96	«Газпром газэнергосеть гелий»	21	«Узбектелеком»	7
Graphite GTC	70	PlayGiga	82	«Газпром»	19, 20, 21	«Узинфоком»	7
GreenMDC	9	Playkey	82	«ГрандМоторс»	9	Университет Инха (Ташкент)	7, 8
Guentner	58, 59	Positive Technologies	79	ДАТАРК	9	«Холдинг ОСК групп»	9
Hatch Entertainment	82	Progress Kinvey	70	ДФУ	21, 22	ЦИК	11
Hitachi	44	Pure Storage	46, 47	«Ди Си Квадрат»	9	«Элемент»	21
HPE	16, 43, 44, 46, 47, 52	Qrator Labs	89, 91	Судостроительный комплекс «Звезда»	19	«Яндекс»	24, 72, 73, 74, 77
HTS	58, 59	Raritan	39				
Huawei	5, 6, 23, 36, 46, 73, 83	RCCPA	77, 75				
IBM	44, 51, 69, 72, 77	Red Hat	69, 70, 72				
IDC	14, 42, 44, 46	Rittal	6, 11, 37, 38, 48, 49				
IDG	53	Safe Host	91				
IEC	63	Salesforce	69, 70, 76				
Igneous Systems	47	Samsung	33				
iKS-Consulting	4, 7, 8, 9, 10, 11, 13, 18, 71, 72, 73, 75, 76	SAP	51				

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.



М Е Д И А

8-я международная конференция

**DATA CENTER
DESIGN & ENGINEERING**

21 мая 2020

• Москва •

Центр Digital October

Реформа

16+

**За дополнительной информацией обращайтесь
по тел.: (495) 150-64-24**

www.dcdforum.ru

CLOUD & DIGITAL

TRANSFORMATION

ИКС

МЕДИА

9-я международная конференция и выставка

ПЕРЕОСМЫСЛИ
БИЗНЕС

26 марта 2020

Москва ❖ Центр Digital October

www.cloud-digital.ru

Реклама

16+