Деловой журнал | ИТ • Телеком • Медиа | www.iksmedia.ru

ИнформКурьер-Связь

ИКС

издается с 1992 года

№ 3 2018

ЦОД в Удомле 8
Сертификация LEED и DGNB 23
Секреты разработки концепции ЦОДа 38
Транспорт для 5G 65
Контейнеры как новый облачный тренд 86

ТЕМА НОМЕРА

ЦИФРОВОЙ КОНТУР МЕДИЦИНЫ

Международная конференция и выставка

«ЦОД-2018: модели, сервисы, инфраструктура»

28 ноября 2018, 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?

При поддержке

Uptime Institute™

Организатор:

ИКС МЕДИА

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

DATALINE · RITTAL · HUAWEI · 3data Premium Data Centers · CABERO HEAT EXCHANGER · ПОЖТЕХНИКА · C3 SOLUTIONS КАЧЕСТВЕННО.СДЕЛАНО.В РОССИИ. · softline · POWERCONCEPT ПРОМЫШЛЕННЫЕ АККУМУЛЯТОРЫ · netangels · socomec Innovative Power Solutions · ПРЕОРА

Издается с мая 1992 г.

Издатель
ООО «ИКС-Медиа»

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

Обозреватели
А.Е. Крылова, Н.В. Носов

Корректор
Е.А. Краснушкина

Дизайн и верстка
Е.В. Денисова

КОММЕРЧЕСКАЯ СЛУЖБА
Г. Н. Новикова, коммерческий директор – galina@iks-media.ru
Ю. В. Сухова, зам. коммерческого директора – sukhova@iks-media.ru
Е.О. Самохина, ст. менеджер – es@iks-media.ru
Д.А. Устинова, менеджер по работе с ключевыми клиентами – ustinova@iks-media.ru
Д.Ю. Жаров, координатор – dim@iks-media.ru

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

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

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

№3/2018 подписан в печать 29.10.18.
Тираж 8 000 экз. Свободная цена.
Формат 64x84/8

ISSN 0869-7973

12+

Edge Cure

Как заявляют эксперты, мнения которых собрала обозреватель ИКС Александра Крылова, мы уже прошли этап формирования «электронного здравоохранения» и приступили к построению «цифровой медицины». Насколько ощутили это рядовые пациенты? По моим наблюдениям, равно как и по впечатлениям моих знакомых, ситуация лучше не стала. Когда недавно я посещал поликлинику, врач уделила мне максимум минуту-две, а потом минут десять что-то ожесточенно печатала на компьютере. Компьютеры установили, сети протянули, но сколько-нибудь полезного обмена электронной информацией даже в рамках одного медучреждения, не говоря уже об обмене данными между клиниками, не наблюдается.

Другая проблема – централизация медицинской экспертизы и ресурсов. Нам ли, много лет занимающимся вопросами цодостроения, не понимать все плюсы такого подхода. Но вот незадача. Недавно счетная палата отметила увеличение младенческой смертности в девяти регионах, где были построены централизованные перинатальные центры. И я не удивлен. В моем родном подмосковном наукограде с населением более 60 тыс. человек закрыли прекрасный роддом. Надо ездить в районный центр. Вроде недалеко, но постоянные пробки превращают такие поездки в кошмар.

Поскольку улучшения дорожной ситуации не просматривается, то для решения поставленной Президентом РФ задачи повышения ожидаемой продолжительности жизни необходима децентрализация, приближение квалифицированной помощи к пациентам. По аналогии с теми же ЦОДами, своего рода Edge Cure, гибридный подход.

Чем могут помочь современные ИТ? Вот лишь один пример. Недавно, когда я покупал в аптеке относительно недорогой препарат, мне в подарок вручили фитнес-браслет от того же производителя. Пройдет совсем немного времени, и вместе с таблетками мы будем получать интернет-гаджеты, отслеживающие температуру, пульс, давление и другие показатели. Производители, страховые компании, медицинские учреждения смогут контролировать наше состояние (надеюсь, предварительно получив наше согласие), чтобы проактивно рекомендовать те или иные процедуры или препараты. И тогда действительно можно будет говорить о поддержании здоровья, а не о запоздалом лечении. Хочется надеяться, что к 2030 году большинство россиян будут жить до 80 лет и даже дольше.

Крепкого вам здоровья,
Александр Барсков

1 КОЛОНКА РЕДАКТОРА

4 ИКС-Панорама

4 Какие ЦОДы нужны новой экономике?
8 ЦОД-гигант на озере Удомля
10 Рынок ЦОДов: цели и стимулы роста
14 Чем ИТ могут помочь частным клиникам в конкуренции?
16 КАЛЕНДАРЬ СОБЫТИЙ

18 Экономика и бизнес

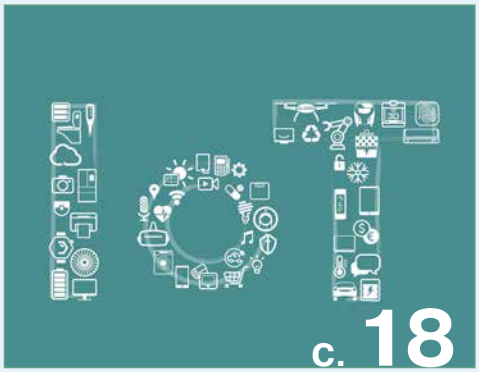
18 Т. Толмачева. ProIoT: «как много в этом звуке…»
23 Д. Кузнецов. Сертификация устойчивого развития: что, как и зачем
28 С. Смолин. Правовой риск-менеджмент в дата-центре

30 Инфраструктура

30 А. Крылова. Оптимизация для цифровой трансформации
36 Д. Анциферов. Быть лидером
38 А. Павлов, Д. Басистый. Разработка концепции ЦОДа. Шаг за шагом
44 В. Новиков. Итальянцы в России
46 А. Эрлих. Кругом вода, или Соблюдение коридора влажности в системах круглогодичного фрикулинга
50 А. Ивашов, А. Крюков. Управление жизненным циклом для изменяющихся инфраструктур
52 А. Краснов. Мультиоблако: новый подход к построению ИТ-инфраструктуры

Какие ЦОДы нужны новой экономике?

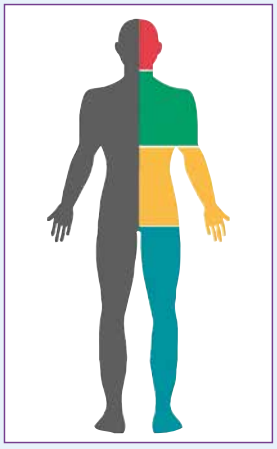
Чем ИТ могут помочь частным клиникам в конкуренции?



Т. Толмачева. ProIoT: «как много в этом звуке…»

с. 30

А. Крылова. Оптимизация для цифровой трансформации



с. 81

И. Шадеркин. Интернет медицинских вещей в профилактических целях

Т. Чирков. ЦОД как сейф

с. 88

54 К. Бобылев. Rittal делится экспертизой с российскими заказчиками

56 Н. Носов. Российский рынок серверной виртуализации: тенденции и игроки

60 «Зеленый» ЦОД в Алабушево

62 С. Орлов. Вычисления на границе

65 А. Абрамов. Транспортные сети 5G. Когда ответы неочевидны

67 Н. Носов. Новые кабельные решения для ЦОДов

69 А. Семенов. СКС категории 8 и 25G Ethernet

72 Сервисы и приложения

72 А. Крылова. Медицина обретает цифровой контур

74 Г. Лебедев. Экспертным системам нужна верификация

76 Т. Зарубина. Если МИС МО не облегчает работу врача – значит, что-то не так с системой

78 Б. Зингерман. От электронных документов – к цифровым сервисам

79 М. Плисс. Частная медицина в ожидании консолидации

81 И. Шадеркин. Интернет медицинских вещей в профилактических целях

83 Н. Носов. Облачные провайдеры помогут в разработке блокчейн-решений

86 А. Захаров. Контейнеры как новый облачный тренд

88 Безопасность

88 Т. Чирков. ЦОД как сейф

92 Н. Носов. Что угрожает безопасности ЦОДа?

94 НОВЫЕ ПРОДУКТЫ

Какие ЦОДы нужны новой экономике?

Курс российского государства на формирование цифровой экономики, возведенный в ранг национального проекта, не может не оказать влияния на темпы роста отрасли центров обработки данных. Чего ожидать игрокам этого растущего рынка?

Об этом шли дискуссии на 13-й международной конференции «ЦОД-2018», организованной «ИКС-Медиа». В нынешнем году мероприятие, являющееся основной российской площадкой для тех, чья профессиональная деятельность связана с дата-центрами, посетили более 800 делегатов.

Разность потенциалов. Развитие информационной инфраструктуры цифровой экономики в госпрограмме, а затем и в одноименном национальном проекте выделено в отдельное направление. На его финансирование с 2018 по 2024 гг. государство планирует направить порядка триллиона рублей – такие данные привел Станислав Мирин, ведущий консультант iKS-Consulting.

По его убеждению, пристальное внимание авторов документа к инфраструктурной составляющей цифровой экономики должно способствовать привлечению публичного интереса к сегменту центров обработки данных, популяризации коммерческих ЦОДов и их услуг, развитию гособлака в интересах органов исполнительной власти всех уровней, а также генерации потребности госорганов в облачной инфрастуктуре.

Минувший год индустрия ЦОДов завершила с 34,4 тыс. стоек, продемонстрировав 13%-ный рост. К концу текущего года количество стоек в коммерческих дата-центрах увеличится на 39,9%, а рост ускорится до 14,5%. Объем рынка коммерческих ЦОДов в денежном выражении, как ожидает аналитик, вырастет с 22 млрд руб. (по итогам 2017 г.) до 27 млрд руб.

Интересно, что в несколько раз быстрее рынка в России растут сертифицированные центры обработки данных. Так, в ЦОДах с подтвержденным уровнем надежности Tier III количество стойко-мест увеличилось за 2017 г. на 31%.

Понятно, что активный ввод в эксплуатацию новых стоек не может не сказываться на утилизации стойко-мест в дата-центрах. Как отметил С. Мирин, несмотря на их переизбыток в сегменте colocation, утилизация снизилась только на 1%, а доходы, которые провайдеры получают с одной стойки, не изменились. Более того, по темпам роста оба сегмента российского рынка ЦОДов – услуг colocation и IaaS (у нас 60% поставщиков инфраструктуры по сервисной модели – это дата-центры) – примерно на пять процентных пунктов опережают весь мир.

Ключевые цели госпрограммы «Цифровая экономика РФ», которые перекочевали и в одноименный национальный проект, – обеспечить развитие отрасли ЦОДов, в том числе за счет экспортно-ориентированных услуг хранения и обработки данных и облачных сервисов, и увеличить долю России в мировом объеме оказания услуг хранения и обработки данных. По словам Видии Железнова, директора по стратегии и маркетинговым коммуникациям «Ростелеком-ЦОД», госпрограммой предусматривалось, что до 2024 г. доля нашей страны в этом сегменте мирового рынка должна вырасти в 10 раз – с 1 до 10%, однако при формировании национального проекта «Цифровая экономика» этот целевой показатель был снижен до 5%.

По итогам 2017 г. на мировом рынке услуг colocation и облачных сервисов с большим опережением лидировали США, на долю которых приходилась почти половина его объема. Россия же, где участники отрасли ЦОДов ориентируются преимущественно на внутренний рынок, пропустила вперед не только Китай, но и Гонконг, а также Сингапур и Индонезию, которые наращивают экспортную активность.

До 1 декабря 2018 г. Министерство экономического развития РФ собирает предложения по снятию административных барьеров, сдерживающих рост экспорта услуг дата-центров. Что это за барьеры? Бумажный документооборот, в том числе в экспортных контрактах, сложный процесс администрирования валютных сделок с нерезидентами, а также обременительные процедуры подтверждения факта и места оказания дата-центром экспортной услуги для возврата и взаимозачета НДС.

Кроме того, предполагается, что Российский экспортный центр

включит индустрию ЦОДов и облачных сервисов в список приоритетных экспортных отраслей и начнет популяризировать и продвигать услуги российских провайдеров по собственным каналам и через сеть торговых представительств за рубежом. Согласно расчетам аналитиков, в случае успеха общий объем трансграничных услуг российских центров обработки данных в 2024 г. составит $65 млн.

Целевой сценарий для повышения доли России на мировом рынке ЦОДов с 1 до 5% – создание виртуальной особой экономической зоны. Сегодня по закону об ОЭЗ компания должна быть резидентом в каком-либо географическом регионе. Но поскольку предоставлять облачные сервисы и услуги colocation можно из любой точки мира, предъявлять такое требование к провайдерам излишне. Им достаточно «получить прописку» в виртуальной особой экономической зоне. Преодолев определенные фильтры, они получат все льготы, которые доступны сегодня резидентам традиционных ОЭЗ: налоговые, административные и регуляторные, а также институциональную и методическую поддержку.

Все вышеописанные мероприятия вошли в новый федеральный проект «Поддержка экспортных услуг» (т.е. относятся не только к индустрии дата-центров), утвержденный 1 октября в одном пакете с Национальным проектом «Цифровая экономика».

От центра – к периферии. Процессы цифровизации всех отраслей экономики требуют предоставления множества электронных услуг и сервисов конечным пользователям – бизнесу и гражданам – с минимальной задержкой, недостижимой при общепринятой централизованной архитектуре дата-центров.

Для формирования цифровой экономики нужно переместить часть вычислительной инфраструктуры ближе к точке генерации и потребления контента из облака, воплотив в жизнь концепцию периферийных вычислений (Edge Computing). Являясь, по сути, высокопроизводительным мостом между потребителями и центральным облаком, edge-компьютеры ускоряют доставку им приложений и сервисов, а также широковещательных данных.

Периферийные вычисления предполагают выстраивание трехуровневой распределенной архитектуры, состоящей из головного ЦОДа, нескольких региональных и множества локальных ЦОДов, констатировал Роман Шмаков, вице-президент подразделения IT Division компании Schneider Electric. По его мнению, при такой архитектуре оснащать по последнему слову техники нужно не только головной ЦОД, но и объекты двух других уровней. В устойчивости и работоспособности периферийные дата-центры не должны уступать основным.

Более того, в понимании компании Schneider Electric само значение термина «неисправности» применительно к дата-центрам должно измениться. Вместо нарушения работы ИТ-оборудования в каком-либо ЦОДе оно должно означать прерывание работы пользователя, включая потерю связи в локальных микроЦОДах. В новых условиях вендор рекомендует провайдерам обеспечивать для всей периферийной инфраструктуры физическую защиту; мониторинг, дистанционный контроль, управление и автоматизацию; резервирование систем электропитания и охлаждения; параллельное обслуживание и резервирование каналов связи.

Для оснащения локальных дата-центров известные мировые производители рекомендуют использовать собранные и протестированные в заводских условиях комплексные решения – сейфовые, контейнерные и капсульные. В частности, компания Rittal, как сообщил Артур Руссманн, ее руководитель международных проектов в странах СНГ, Прибалтики и Австрии, разработала сценарии применения edge-ЦОДов в «умном» ритейле, «умных» телекоммуника-

циях, «умном» здравоохранении, на «умных» предприятиях и для «умных» дорог с автономными автомобилями. Каждое комплексное решение edge-ЦОДа, задействованное в том или ином сценарии, максимально соответствует запросам этих отраслей цифровой экономики по объему данных, доступности сервисов, задержке, безопасности и стандартизации. Это позволяет компаниям получать вычислительные мощности рядом с местом, где сосредоточены данные, причем максимально быстро и безопасно.

При этом по мере распространения периферийных вычислений будет изменяться спектр задач, которые решает центральное облако. В его зоне ответственности, как указывает А. Руссманн, остаются координация работы узловых дата-центров всех уровней, агрегация данных, их анализ, обработка и архивация данных бэк-офиса.

Российские производители тоже готовы участвовать в реализации концепции Edge Computing, предлагая надежные и экономичные решения для головных ЦОДов. К примеру, в портфеле компании ДКС можно найти высоконадежные источники бесперебойного питания, трансформаторы, телекоммуникационные и серверные шкафы, СКС, системы лотков и монтажных креплений, а также шинопроводы.

Облака ждут новых пользователей. Пока же услуги на базе облачных технологий становятся все популярней, как у клиентов, так и у дата-центров. И этот интерес совпадает с вектором развития цифровой экономики.

«Ростелеком-ЦОД», который планирует к 2020 г. довести число стоек в своих дата-центрах до 12 тыс., активно развивает все основные варианты облачных сервисов: IaaS, SaaS и PaaS. Как рассказал Евгений Сбитнев, директор департамента исследований и разработки новых продуктов «Ростелеком-ЦОД», в рамках развития SaaS-сервисов компания тестирует большое число отечественных программных продуктов, позволяющих реализовать «рабочее место как сервис». Также в планах компании разработка сервисов аварийного восстановления (Disaster Recovery as a Service), резервного копирования (Backup as a Service), баз данных как сервис (Database as a Service) и облачного файлового хранилища. Кроме того, в компании работают над сервисом виртуализации графических ядер.

Внедрение в публичном облаке сложных многофункциональных систем, таких как SAP HANA, с одной стороны, обеспечивает существенный выигрыш в скорости развертывания, гибкости, экономичности, надежности и удобстве администрирования. С другой стороны, для того чтобы внедрение прошло гладко, от команды, его осуществляющей, требуется владеть специальными инструментами, к примеру, SAP Quick Sizer (HANA/Classic), позволяющими на этапе проработки архитектуры будущего решения не ошибиться с объемом необходимых ресурсов. Эксперты инфраструктурной практики компании Accenture, которая оказывает консалтинговые услуги по миграции на SAP HANA и SAP Basic, рекомендуют обращать внимание на лицензирование операционных систем, используемых для развертывания SAP, обязательно уточнять у провайдера условия подписки на сервис (модель оплаты, список готовых имиджей ОС и список сервисов Azure). Также проверке подлежат безопасность и легальность хранения персональных данных и техническая поддержка, которую берется обеспечить провайдер услуг.

По цифровому Шелковому пути. Для того чтобы вписаться в глобальную цифровую экономику, России предстоит задействовать как внутренние, так и внешние источники, считает Гай Вилнер, соучредитель и генеральный директор дата-центра IXcellerate.

По его убеждению, принятие на себя роли цифрового Шелкового пути, консолидация рынка и строительство новых объектов, применение передовых мировых практик, использование технологий интернета вещей в сочетании с зарубежными инвестициями должны стать новыми драйверами развития российского рынка ЦОДов в эпоху перехода к цифровой экономике.

По словам Г. Вилнера, Москва уже начинает восприниматься соседями как узел транзита из Азии в Европу. Количество компаний из Поднебесной, появившихся за последние два года на российском рынке, дает основания говорить об экспансии китайских компаний. К известным производителям телекоммуникационного и ИТ-оборудования добавились операторы связи, банки, участники рынка электронной коммерции. Кстати, China Unicom и Чайнасельхозбанк выбрали поставщиком услуг ЦОДа в России компанию IXcellerate.

В основании цифровой экономики лежат экосистемы и платформы, и на рынке ЦОДов и облачных услуг они в ближайшем будущем тоже появятся. Результатом совместного развития разных участников должны стать повышение надежности объектов и доступности сервисов, ускорение транзакций и более низкие цены.

Александра Крылова

ЦОД-гигант на озере Удомля

«Росэнергоатом» представил специалистам первые секции крупнейшего в России ЦОДа – головного в сети дата-центров проекта «Менделеев». Объект реализован вблизи Калининской АЭС.

ЦОДы – одни из крупнейших потребителей энергии: в 2017 г. все дата-центры в мире потратили примерно столько же электричества, сколько такая огромная страна, как Россия. Поэтому идея размещать эти объекты вблизи крупных электростанций давно витает в воздухе. Концерн «Росэнергоатом» в партнерстве с ПАО «Ростелеком» реализовал эту идею, построив в г. Удомля крупнейший ЦОД в России, который также является одним из самых больших в Европе.

По состоянию на конец сентября 2018 г. в рамках первой очереди проекта возведены административный корпус и три здания с серверными залами. В каждом здании – восемь залов вместимостью порядка 200 стоек каждый. Первый зал, где уже установлена часть ИТ-оборудования, будет использоваться «Росэнергоатомом» для собственных нужд. Еще три зала в том же здании концерн планирует задействовать для коммерческих целей. Остальные залы первой очереди поступят в распоряжение «Ростелекома».

Вторая очередь проекта на данный момент представляет собой площадку для размещения модульных и контейнерных ЦОДов. Срок реализации этой очереди – III квартал следующего года. Предполагается, что после ввода в эксплуатацию второй очереди емкость всего центра составит порядка 7760 стойко-мест.

Бесперебойное гарантированное энергоснабжение ЦОДа обеспечивают Калининская АЭС и собственная система электропитания. Подведенная мощность первых секций – 48 МВт. В перспективе запланировано наращивание мощности ЦОДа до 80 МВт.

Как отмечает Сергей Мигалин, заместитель генерального директора – директор по экономике и финансам АО «Концерн Росэнергоатом», поскольку в АЭС резервирование осуществляется на уровне ее энергоблоков, а сама станция через сеть ФСК включена в единую энергосистему, то перебои с поставкой электроэнергии практически исключены. Очистку поступающего в ЦОД электричества и дополнительный уровень резервирования обеспечивает система динамических ИБП.

Размещение объекта рядом с АЭС имеет немало конкурентных преимуществ. Это, в частности, минимальные оптовые цены на электроэнергию – используется тариф, по которому она покупается станцией для собственных нужд, отсутствует сбытовая надбавка. Кроме того, минимизированы затраты на технологическое подключение, поскольку распределительные устройства и подстанции уже установлены.

Расположение ЦОДа на охраняемой территории рядом с АЭС гарантирует высочайший уровень защищенности,

Слева – возведенные корпуса 1-й очереди, справа – площадка под модульные и контейнерные ЦОДы 2-й очереди

Один из серверных залов ЦОДа

На переднем плане – выхлопные трубы динамических ИБП ЦОДа, на заднем – градирни Калининской АЭС

Система охлаждения – традиционная, с чиллерами на крыше

который обеспечивается стратегическим государственным объектам и вряд ли доступен «обычным» ЦОДам. Упомяну хотя бы то, что зона вокруг АЭС является бесполетной с соответствующими средствами защиты.

На базе ЦОДа в Удомле планируется предоставлять весь спектр услуг коммерческих дата-центров. Это, конечно, традиционные услуги размещения оборудования, включая аренду индивидуального аппаратного зала, а также контейнерное размещение. Кроме того, планируется предложить облачные сервисы (в первую очередь IaaS), организацию резервных ЦОДов, сервисы информационной безопасности и пр.

Выход на рынок коммерческих ЦОДов столь масштабного нового игрока, да еще с очевидными конкурентными преимуществами в части привлекательной цены электричества и повышенной защищенности, способен стать дополнительным катализатором развития ИТ-аутсорсинга, в первую очередь для государственных заказчиков. Правда, традиционно КЦОДы в России тяготеют к двум столицам, а новый ЦОД-гигант разместился практически посередине. И хотя «сапсаны» существенно сокращают время поездки в этот ЦОД из Москвы или Санкт-Петербурга, службам маркетинга «Росэнергоатома» и «Ростелекома» предстоит непростая работа по преодолению стереотипов заказчиков в части географических предпочтений при выборе площадок для размещения ИТ-ресурсов.

Строительство ЦОДа в Удомле – первый шаг проекта «Менделеев», предполагающего создание целой сети национальных ЦОДов на площадках рядом с АЭС. Цель этого проекта – обеспечение высокой физической и информационной безопасности критически важных данных клиентов, связанных с национальными интересами.

По словам С. Мигалина, площадкой для построения следующего ЦОДа, возможно, станет Кольская АЭС. Кроме того, он отметил заинтересованность «Росатома» в экспорте услуг построения дата-центров. Российская государственная корпорация по атомной энергии занимает первое место в мире по величине портфеля зарубежных проектов (36 энергоблоков в 12 странах). Вполне логично в рамках этих проектов предлагать и создание дата-центров. Синергия дешевой электроэнергии и высокой защищенности делает такие ЦОДы весьма привлекательными, особенно в свете реализации программы «Цифровая экономика РФ».

ЦОДы, подобные тому, что построен в Удомле, могут стать важными элементами реализации экспортного потенциала российской индустрии КЦОДов. По оценкам iKS-Consulting, объем рынка ЦОДов России составляет $350 млн, это всего 0,9% мирового и 2% рынка США. Одной из целей госпрограммы «Цифровая экономика РФ» является увеличение доли России в мировом объеме услуг хранения и обработки данных. По словам Видии Железнова, директора по стратегии и маркетинговым коммуникациям компании «Ростелеком-ЦОД», государственной программой предусматривалось, что до 2024 г. доля нашей страны в этом сегменте мирового рынка должна была вырасти в 10 раз – с 1 до 10%, однако при формировании Национального проекта «Цифровая экономика» этот целевой показатель был снижен до 5%.

Александр Барсков,
Удомля – Москва

Рынок ЦОДов: цели и стимулы роста

Тема развития индустрии ЦОДов в свете реализации программы «Цифровая экономика РФ» красной нитью прошла через всю программу конференции «ЦОД-2018: модели, сервисы, инфраструктура», проведенной «ИКС-Медиа» в Санкт-Петербурге.

Один из целевых показателей, заложенных в программу «Цифровая экономика РФ», – увеличение доли России в мировом объеме оказания услуг хранения и обработки данных к 2024 г. до 5%. А сегодня доля нашей страны не превышает 1%. Согласно государственным планам, отрасли коммерческих ЦОДов предстоит сделать просто гигантский скачок. По оценкам iKS-Consulting, для достижения указанной цели среднегодовой рост должен составить порядка 40%.

Основные причины отставания России от мировых лидеров на глобальном цифровом рынке назвал на конференции в Санкт-Петербурге Игорь Семенихин, врио директора Департамента инфраструктурных проектов Министерства цифрового развития, связи и массовых коммуникаций РФ: это проблемы нормативной базы для цифровой экономики и недостаточно благоприятная среда для ведения бизнеса и инноваций.

Российский рынок КЦОДов стабильно растет – по данным iKS-Consulting, в период 2016–2018 гг. средний ежегодный рост числа стоек составил 14,5%, – но отечественные стандарты оценки КЦОДов отсутствуют. В «дорожную карту», предлагаемую Минкомсвязью для стимулирования развития индустрии ЦОДов, входит ряд мер нормативного правового регулирования. В частности, предполагается разработка стандартов оценки ЦОДов и их сертификация.

В «дорожную карту» включены также прямое стимулирование строительства ЦОДов и развитие внутреннего спроса. Среди мер прямого стимулирования – упрощение процедуры получения земель под строительство, повышение энергетической доступности, налоговые и таможенные льготы, создание виртуальной особой экономической зоны. Меры развития внутреннего спроса, по словам представителя Минкомсвязи, предусматривают популяризацию сервисной модели, стимулирование дата-генерирующих предприятий и отраслей.

От двух столиц – до самых до окраин

Сосредоточение подавляющего числа современных КЦОДов в Москве и Санкт-Петербурге (см. рисунок на с. 12) при их отсутствии в большинстве региональных центров И. Семенихин назвал серьезным перекосом в отрасли. Присутствовавшие на конференции руководители ряда крупнейших столичных КЦОДов рассказали о том, что не раз прорабатывали возможность построения дата-центров в регионах, но экономика проектов «не сходилась». ЦОДы не идут в регионы, считая, что там нет спроса, а спрос не возникает, потому что в регионах нет качественных ЦОДов. Возможно, синергия экспертизы крупнейших бизнес-игроков и мер поддержки, предложенных Минкомсвязью, поможет разорвать этот замкнутый круг, реализовав региональные проекты и обеспечив доступ базирующихся в регионах предприятий и организаций к современным услугам ИТ-аутсорсинга.

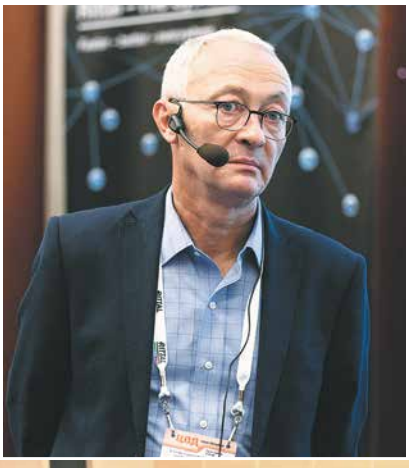
Децентрализация ЦОДов – это общемировая тенденция. Во многом она обусловлена требованиями к снижению времени задержки, которые предъявляют новые приложения, связанные с интернетом вещей, «цифровым» производством, «умными» городами, дополненной реальностью и пр. Для этих приложений задержка должна быть чрезвычайно мала, порядка 1 мс и менее. Для обеспечения такой задержки необходимо, чтобы расстояние от ЦОДа до потребителя его сервисов не превышало 100 км. Следовательно, концентрация ЦОДов в двух столицах означает

невозможность использования их заказчиками из российских регионов для работы чувствительных к задержкам приложений, которых становится все больше.

Надежно, как в сейфе

Свой подход к децентрализации и организации распределенной структуры дата-центров представила на форуме «ЦОД-2018» в Санкт-Петербурге компания Rittal. Александр Кюн, менеджер Rittal по продукции для ИТ-инфраструктуры, предложил разделить ЦОДы на три группы: локальные, периферийные и облачные. «То, что раньше называлось серверной стойкой, теперь – edge- или микроЦОД», – заметил он. Изменение терминологии – это не какая-то маркетинговая блажь, новые термины отражают повышение требований даже к небольшим ИТ-комплексам.

Немецкий производитель предлагает комплексные решения для всех трех категорий ЦОДов. Скажем, для локальных объектов это микроЦОДы, в том числе реализованные как сейфы с защитой от всевозможных факторов риска, будь то пожар, затопление, взлом, воздействие пыли и пр. Такой сейф можно собрать вокруг уже работающего ИТ-оборудования, а несколько модульных сейфов – соединить в единый комплекс.



Гибридные ИБП

Использование заказчиком нескольких ИТ-площадок, – как собственного ЦОДа, так и коммерческого, – означает переход на гибридную схему построения ИТ-инфраструктуры. Интересно, что гибридные решения предлагают и поставщики инженерных систем для ЦОДов. Как рассказал на форуме Владислав Ротань, директор по развитию бизнеса и продажам компании Piller, ее решения позволяют задействовать в качестве системы накопления энергии в динамическом ИБП как «родной» для этого типа устройств маховик, так и классические аккумуляторные батареи (АКБ). Возможна и обратная ситуация, реализованная в системах ActivePower, когда для кратковременного автономного питания нагрузки в статическом ИБП применяются не аккумуляторы, а маховик. Это решение снижает планку использования маховиков до 225 кВт – именно на такую мощность рассчитана модель ActivePower CleanSource 225XT.

Компания Piller также разработала технологию IP-Bus, которая позволяет реализовать схемы отказоустойчивости Tier IV с уровнем резервирования N + 1 (а не 2N), что существенно снижает расходы на инженерное оборудование. IP-Bus – это специальная схема включения динамических ИБП с внешними ДГУ на общую шину. Такая конфигурация уже реализована в нескольких ЦОДах, например, на объекте NEXTDC B2 (Австралия), который сертифицирован организацией Uptime Institute по уровню Tier IV Design & Facility. А в ЦОДе Hana Financial Group (Южная Корея) мощностью 12,7 МВт в схеме IP-Bus динамические ИБП сочетаются с литий-ионными батареями. Это еще один пример построения гибридной системы бесперебойного гарантированного электропитания, которая по совокупности причин оказалась для южнокорейского заказчика оптимальной.

Когда облаков становится много

Помимо децентрализации ЦОДов, важным трендом является быстрое развитие облачных сервисов, которые по темпам роста существенно опережают другие услуги, предоставляемые на базе коммерческих ЦОДов. Сегодня большинству компаний уже понятны преимущества мультиоблачного подхода (так называемого мультиклауда), вопрос в том, как наилучшим образом реализовать соответствующие схемы. Важным в решении этого во-

проса Сергей Халяпин, главный инженер Citrix в России и странах СНГ, считает удобство и простоту интеграции имеющихся в компании ИТ-ресурсов и приложений с выбранной облачной моделью. Для того чтобы облегчить такую интеграцию, Citrix реализовала поддержку всех основных гипервизоров (включая системы VMware, Microsoft, KVM и его разновидности), а с помощью коннекторов – подключение к наиболее популярным публичным облакам (AWS, Microsoft Azure, Google Cloud, Rackspace и др.).

Не менее важна для пользователя уверенность в безопасности работы в публичном облаке. Рассматривая этот вопрос на примере близких ему решений, С. Халяпин отметил, что «у Citrix Cloud нет доступа к корпоративным данным заказчиков». Образы машин и данные приложений всегда размещаются на выбранной заказчиком площадке, а Citrix Cloud сохраняет только метаданные пользователей и приложений.

Как преодолеть «кризис управления»

Доступность и удобство пользования сервисами из облака – очевидные катализаторы дальнейшего развития ИТ. Однако традиционные подходы к управлению при быстром росте количества серверов могут стать тормозом такого развития. Кирилл Степанов, системный инженер компании SUSE, предлагает несколько путей выхода из «кризиса управления»:

- автоматизация развертывания – переход от традиционных способов установки приложений к запуску предварительно настроенных контейнеров;
- автоматизация масштабирования – реализация служб и приложений в виде набора микросервисов;
- полная автоматизация управления запуском и выполнением контейнеров – оркестрация, самовосстановление, самообслуживание пользователей.

Задачи управления эффективно решаются на основе программно определяемой инфраструктуры. В SUSE предпочитают термин «программно реализуемая инфраструктура» и ратуют за использование для такой инфраструктуры свободного ПО. Помимо технологических (быстрое совершенствование кода сообществами разработчиков, открытые стандарты), представитель SUSE указывает и на экономические преимущества свободного ПО. Гибкость выбора конфигурации и возможность использования «стандартной» (недорогой) аппаратуры позволяют значительно снизить капитальные затраты. При этом полностью устраняется зависимость от технологической и ценовой политики единственного изготовителя.

Компания HPE предлагает свой вариант решения задачи управления серверными ресурсами на основе новой программно определяемой платформы HPE Synergy. Конструктивно платформа представляет собой шасси, куда устанавливаются все необходимые модули: вычислители, СХД, сетевая фабрика. Все компоненты построены по принципу «программной определяемости», а для управления инфраструктурой в составе HPE Synergy имеется специальный компоновщик – сервер с ПО OneView.

Запомнить все

Развитие ИТ неразрывно связано с ростом требований к системам хранения данных. В этой области наиболее активно сегодня развиваются решения на базе флеш-памяти (SSD). Представляя рекомендации Fujitsu, Денис Макашов, менеджер этой компании по работе с партнерами в СЗФО, советует перевести большую часть инфраструктуры систем хранения на технологию SSD как более эффективную альтернативу HDD.

Что касается вопросов надежности, то здесь эксперт Fujitsu рекомендует полагаться на кластеры с синхронной репликацией данных. «Даже много девяток, характеризующих готовность одного узла, – это еще не гарантия доступности сервиса», – подчеркнул он.

■ ■ ■

В целом возможность приобретения российскими компаниями самых современных технических решений наряду с глубокой экспертизой ее специалистов и разработанными государством мерами стимулирования отрасли – важное условие роста индустрии центров обработки данных.

Александр Барсков,
Санкт-Петербург – Москва

Discover the Edge.

Smart Solutions. Real Business.

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

RITTAL

FRIEDHELM LOH GROUP

www.rittal.ru

Чем ИТ могут помочь частным клиникам в конкуренции?

Три-четыре года назад инвестировать в медицинский бизнес стало модным, но любая мода проходит, а клиникам, число которых выросло, приходится конкурировать между собой. Как с помощью информационных технологий побеждать в конкурентной борьбе?

Ситуация на рынке вынуждает сегодня собственников и руководителей медицинских учреждений задумываться о средствах повышения устойчивости своего бизнеса. А ее, как заявил на Форуме руководителей медицинских учреждений «Конкуренция в медицине» Павел Бранд, медицинский директор сети клиник «Семейная», лучше всего описывают такие показатели, как «оставляемость» пациентов, их «возвращаемость» и «направляемость». С помощью первого показателя оценивается удовлетворенность пациентов первичным приемом в клинике и готовность продолжить с ней отношения. Второй параметр характеризует готовность хронических больных оставаться под наблюдением лечащего врача и приходить к нему на прием каждые два-три месяца. Третий – говорит о согласии пациента с направлением его к другим врачам клиники и на дополнительные обследования.

Иными словами, об устойчивом росте медицинского бизнеса можно говорить только при наличии теплых личных контактов между клиникой и пациентом. При этом, как показали дискуссии, добиться от пациентов положительного отношения к клинике руководителям медорганизаций не так-то легко. «Пациенты отнюдь не глупы и видят, когда их “разводят на деньги”», – констатировал Алексей Парамонов, управляющий партнер и генеральный директор клиники «Рассвет», добавив, что «сарафанное радио» работает хорошо, причем особенно быстро разносятся негативные отзывы.

Наиболее «продвинутые» инвесторы и управленцы медучреждений находятся в поиске современных ИТ-решений и разнообразных электронных сервисов, позволяющих оптимизировать рутинные процессы и сокращать затраты. «Пока информационные технологии по большей части используются для обеспечивающих основную деятельность клиники подразделений – бухгалтерии, маркетинга, регистратуры, – констатировал А. Парамонов, – врачи с ними сталкиваются намного реже». По его словам, ситуация изменится, когда распространение получат системы поддержки принятия врачебных решений.

В. Коршок: «Сервисная оболочка должна быть незаметной для пациента, простой и удобной».

Сегодня в клинике «Рассвет» внедрена и развивается медицинская информационная система «Элемент». Ее функционал скоро пополнится интеллектуальным модулем для проверки назначаемых врачом лекарств на наличие среди них конфликтующих препаратов. Кроме того, в ближайшее время пациенты смогут воспользоваться мобильным приложением, позволяющим записаться на прием, получить доступ к своей электронной медкарте и т.д.

Позитивный эффект – повышение привлекательности для клиентов – дает автоматизация «сервисной оболочки» клиники, считает Владимир Коршок, заместитель генерального директора по клинико-экспертной работе, главный врач сети клиник «Чайка», поскольку в этом случае пациентам обеспечивается быстрый и безбарьерный доступ к лечащему врачу.

Пациенты клиник «Чайка» на протяжении четырех лет имеют возможность на сайте этого медучреждения вносить свою запись на прием сразу в расписание врача. «Этот сервис работает хорошо: 45% наших пациентов записываются через сайт, не вступая в контакт с регистратурой. В выручке это более 30%», – подчеркнул В. Коршок. При этом доля пациентов, которые таким образом записываются на прием, а потом не являются на него, по его словам, не отличается от доли не пришедших пациентов, записавшихся к врачу по телефону.

При усовершенствовании сервисной оболочки можно ориентироваться на известные услуги, работающие поверх интернета: заказ такси, еды, билетов на развлекательные мероприятия, адаптируя

хорошо зарекомендовавшие себя технические решения, например чат-боты, к бизнес-процессам медицинских учреждений.

В клиниках автоматизированные системы, способные общаться с клиентами на понятном им языке, выбирая ответы из базы данных, могут существенно разгрузить администраторов и регистраторов, в чьи обязанности входит сбор подтверждений явки у записавшихся на прием пациентов, убежден Максим Куимов, генеральный директор компании «Амнисс». Традиционный путь – от записи до явки пациента на прием – требует от администратора совершить два-три звонка, а ведь таких пациентов бывают десятки.

Практика показывает, что чат-бот, «живущий» в популярных мессенджерах, разгружает администраторов медучреждений на 70–80%. Так, за день до приема, на который записан пациент, чат-бот отправит ему сообщение с просьбой подтвердить запись, нажав на кнопку «да» или «нет». Если клиент отвечает отрицательно, чат-бот предложит ему перенести запись в пределах месяца–выбрать и указать новые дату и время визита, а затем запросит подтверждение этой операции. Таким образом пациент избавляется от необходимости отвлекаться на телефонный разговор с администратором, а клиника решает свою задачу.

Уже сегодня медицинские организации, которые не внедряют инновации, сталкиваются с такими негативными последствиями, как финансовые потери, невозможность управлять качеством сервиса, отсутствие в портфеле программ удаленного сопровождения пациентов, к примеру телемедицинских консультаций, указал Александр Константинов, генеральный директор компании ONDOC. Он порекомендовал медицинским учреждениям, которые хотят быть конкурентными, обратить внимание на сервис личного кабинета, в основе которого лежит решение, соответствующее требованиям информационной безопасности и защиты персональных данных.

Пациенту этот сервис помогает записаться на прием и с помощью push-уведомления, т.е. бесплатно, напоминает о записи, о необходимости принять лекарство, пройти повторное обследование, предоставляет удаленный доступ к медкарте. А клиника может использовать его как дополнительный канал коммуникаций, направляя в него сообщения о маркетинговых акциях и скидках.

Словом, участники форума могли убедиться, что насыщение частных медицинских клиник современными ИТ-решениями и сервисами позволяет им повысить лояльность пациентов и культуру взаимоотношений с ними. А она тоже очень важна для повышения конкурентоспособности.

Александра Крылова

Еще больше о роли ИТ в современном здравоохранении – в теме номера (с. 72—82).

8 ноября в Москве (отель «Рэдиссон Славянская») состоится **11-й CNews Forum 2018: «Информационные технологии завтра»**.

Цель мероприятия – предоставить независимую площадку для обсуждения ключевых вопросов и актуальных проблем рынка ИКТ, инновационных технологий, подходов к реализации ИТ-проектов с участием трех сторон – бизнеса, ИТ-поставщиков и государства.

Программа CNews Forum 2018 состоит из двух частей: в первой состоится пленарное заседание с участием экспертов мирового уровня, ключевых представителей российского бизнеса и госсектора, во второй делегатам будут доступны тематические секции: «Госсектор», «Безопасность», «Розница», «Банки», «Business Intelligence и большие данные», «Фарминдустрия» и «Облачные технологии».

На сессионных заседаниях будет представлена информация о наиболее перспективных ИТ-решениях, а также об инновационных проектах, реализуемых в соответствующих отраслях.

В рамках форума пройдет церемония награждения CNews Awards, призванная отмечать максимально эффективные достижения в области ИТ за прошедший год. Выбрать победителя можно будет путем онлайн-голосования во время мероприятия.

Организаторы: CNews Conferences, CNews Analytics.

forum.cnews.ru/2018

выставки, семинары, конференции

Дата и место проведения, организатор, сайт	Наименование мероприятия
08.11. Москва **CNews Conferences** forum.cnews.ru	CNews Forum 2018: «Информационные технологии завтра»
09.11. Москва **ИКС-МЕДИА** itmedforum.ru	**5-я ежегодная конференция и выставка IT & Med'2018**
13.11. Москва **Международная ассоциация специалистов по управлению клиентским опытом** www.icxc.online	Международный форум Martech Expo Russia 2018
14.11. Москва **Teradata** www.teradata-forum.ru	Teradata Forum 2018
20.11. Москва **«Событие»** sobytie.msk.ru/smartcity	Ежегодный международный форум «Smart City 2018: цифровая трансформация»
20.11. Москва **TelecomDaily** www.tmtconferences.ru/5g2018.html	2-й всероссийский бизнес-форум «Развитие сетей беспроводной связи в России – 5G Future Russia 2018»
21.11. Москва **РАЭК** riw.moscow	11-я Неделя российского интернета (RIW 2018)
22.11. Нижний Новгород **Министерство информационных технологий, связи и средств массовой информации Нижегородской области** it-brandnn.ru	Региональный конкурс в сфере информационных технологий «IT-проект года 2018»
28.11. Екатеринбург **ИКС-МЕДИА** ekb.dcforum.ru	**Международная конференция и выставка «ЦОД-2018: модели, сервисы, инфраструктура»**

Присылайте анонсы ваших мероприятий на IKSMEDIA.RU

Еще больше на

21–23 ноября в Москве (ВДНХ) пройдет **11-я Неделя российского интернета (RIW 2018).**

RIW – это главное ежегодное выставочно-конференционное событие сразу пяти отраслей: интернет, телеком, медиа, технологии, софт.

Мероприятие будет включать в себя:

- Internet FORUM 2018 – более 20 тематических блок-конференций и десятки мастер-классов, в рамках которых с докладами выступят более 700 спикеров, представителей бизнеса, государства, ИТ-сообщества;
- Internet EXPO 2018, экспозицию достижений российских и зарубежных ИТ-компаний, нацеленную как на профессионалов, так и на рядовых пользователей Рунета и цифровых технологий;
- Internet SHOW 2018, демонстрацию возможностей цифровых технологий, презентаций продуктов и технологий в формате RED DOT;
- RIW.NIGHTS, серию внепрограммных культурно-развлекательных мероприятий (премий, презентаций и промоакций).

Организатор: РАЭК.

riw.moscow

С 31 января по 1 февраля 2019 г. в Москве (здание Правительства Москвы) состоится **21-й большой национальный форум информационной безопасности «Инфофорум-2019»**.

«Инфофорум» проводится с 2001 г. и на 10 тематических сессиях собирает более 1,5 тыс. участников практически изо всех регионов России и дружественных стран.

Форум будет состоять из пленарного и тематического заседаний и выставки в здании Правительства Москвы. 1 февраля впервые на «Инфофоруме» пройдут технические сессии крупнейших компаний с посещением их объектов.

В рамках мероприятия состоится награждение лауреатов профессиональной премии в области информационной безопасности «Серебряный кинжал» и всероссийского конкурса студентов и молодых специалистов «Инфофорум – новое поколение».

Соорганизаторами форума выступят комитет Государственной Думы ФС РФ по безопасности и противодействию коррупции и аппарат Совета безопасности РФ.

Организатор: «Инфофорум».

infoforum.ru

выставки, семинары, конференции

Дата и место проведения, организатор, сайт	Наименование мероприятия
29.11. Москва **TAdviser** summit.tadviser.ru	TAdviser SummIT
30.11. – 01.12. Москва **Кластер информационных технологий фонда «Сколково»** sk.ru/foundation/events/november2018/cyberday/p/program.aspx	Skolkovo Cyberday Conference
01.12. Москва ФРИИ iidf.vc/goglobal/2018	Кейс-конференция Russian Startups Go Global 2018
04–05.12. Москва **Координационный центр национального домена сети Интернет** eednsforum.org/ru/	EE DNS Forum 2018
05.12. Москва CNews Conferences events.cnews.ru/events/internet_veschei_2018.shtml	Конференция «Интернет вещей 2018»
05–06.12. Москва **Академия информационных систем (АИС)** vipforum.ru	9-й международный форум «Борьба с мошенничеством в сфере высоких технологий» AntiFraud Russia
11–12.11. Москва **IC ENERGY** icenergy.co.uk/ru/event200.html#remind_frm	Международная конференция «ИТ в ритейле»
29–31.01.2019 Москва **«МидЭкспо»** cstb.ru	21-я международная выставка и форум телевидения и телекоммуникаций CSTB Telecom & Media 2019
31.01–01.02.2019 Москва **«Инфофорум»** infoforum.ru/conference/2019	21-й большой национальный форум информационной безопасности «Инфофорум-2019»

С 30 ноября по 1 декабря в Москве (ИЦ «Сколково») пройдет международная конференция **Skolkovo Cyberday Conference 2018**. Цель конференции – определить новые технологические подходы и решения, призванные обеспечить информационную безопасность в условиях интеграции информационных технологий в ключевые бизнес-процессы компаний. Главные темы нынешнего года: «Будущее кибербезопасности – вызовы и возможности», «Кибербезопасность и искусственный интеллект», «Новые подходы и решения обеспечения информационной безопасности» и «Программа Bug Bounty».

В рамках конференции пройдет турнир по информационной безопасности – II кубок CTF России. Этот проект позволит 20 лучшим региональным командам студентов и школьников, победившим на соревнованиях серии CTF, а также разработчикам CTF-турниров побороться за звание чемпиона страны.

В ходе конференции будет анонсирован Skolkovo Cybersecurity Challenge – международный конкурс инновационных проектов, направленных на защиту бизнеса и частных лиц от киберугроз.

Также в рамках Skolkovo Cyberday состоится межотраслевая конференция «БИТ Москва», посвященная вопросам информационной безопасности.

Организатор: кластер информационных технологий фонда «Сколково».

sk.ru/foundation/events/november2018/cyberday

29 января 2019 г. в Москве («Крокус Экспо») в рамках ежегодного форума и выставки CSTB. Telecom & Media пройдет церемония награждения победителей Национальной премии в области многоканального цифрового телевидения **«Большая Цифра»**.

В 2019 г. премия «Большая Цифра» будет присуждаться в десятый раз. За время, прошедшее с первой церемонии награждения, количество номинантов увеличилось с 50 до 170, а количество номинаций превысило 25.

За десять лет премия подтвердила свою значимость в формировании и развитии цивилизованного рынка многоканального цифрового телевидения в России и странах СНГ. В жюри премии входят журналисты, эксперты в области телерадиовещания, общественные деятели и представители операторов многоканального цифрового ТВ. Со дня основания премии возглавляет профессиональное жюри Анатолий Лысенко, президент Международной академии телевидения и радио, генеральный директор Общественного телевидения.

Отдельно проходит зрительское голосование. Благодаря технической поддержке операторов платного телевидения количество его участников уже перевалило за 100 тыс.

Абонентская база платного телевидения продолжит расти за счет потенциала IPTV и спутникового ТВ. По прогнозу аналитиков, к концу 2018 г. число абонентов вырастет на 1,8%, до 43,5 млн, а проникновение превысит 76%. Объем российского рынка по итогам 2018 г. приблизится к 90 млрд руб.

Российский телевизионный контент активно потребляется за рубежом, в особенности детский мультипликационный. Мы уже стали свидетелями успехов российских дистрибьюторов на латиноамериканском рынке. Интерес к отечественному контенту продолжает расти и в России за счет повышения его доступности на OTT- и VOD-платформах, увеличению количества тематических телеканалов крупных медиакомпаний.

Подать материалы для участия в премии необходимо до 9 ноября. Заявки номинантов заполняются через личный кабинет на сайте премии www.bigdigit.ru, там же размещен список номинаций.

Организаторы: «Мидэкспо», АКТР.

bigdigit.ru

ProIoT: «как много в этом звуке»

Татьяна Толмачева,
партнер, iKS-Consulting

Несмотря на различия в терминологии и функциональных возможностях, во многих отраслях экономики реализуется все больше проектов в сфере интернета вещей.

Термин «интернет вещей» хоть и стал привычным, но даже в рамках одной отрасли для разных компаний его наполнение неодинаково. Причина – в многогранности и многоликости самого рынка. Понятие интернета вещей тесно связано со смежными понятиями – «умными» технологиями, цифровизацией, автоматизацией, а в его решениях, как правило, используются сразу несколько технологий. Именно поэтому часто встречаются некоррелирующие между собой определения и оценки рынка. Это многообразие, вероятнее всего, сохранится и в дальнейшем, либо сам термин трансформируется в новую маркетинговую концепцию.

Рис. 1. Уровень цифровизации отраслей

Проникновение программно-аппаратных средств в разных отраслях сильно различается и зависит от специфики отрасли и степени ее технологичности.

Точка отсчета: где начинается рынок?

Российский рынок уже насыщен разного рода программно-аппаратными системами автоматизации, телеметрии, диспетчеризации, автоматическими системами учета и контроля (рис. 1), которые значительно различаются по функциональным возможностям, топологии, используемым техническим средствам, носителям, протоколам передачи данных и т.д.

Какие технологии можно отнести к интернету вещей? Телематика, телеметрия, диспетчеризация, в том числе и с помощью технологий M2M, давно вошли в нашу жизнь. Где начинаются «продуктовые границы» рынка? Можно выделить два методических подхода.

В рамках первого подхода интернетом вещей считается совокупность физических объектов, объединенная в сеть.

Согласно второму подходу, интернет вещей имеет ряд особенностей, отличающих его от технологий предыдущих поколений, в частности: а) большие масштабы сети; б) интеграция сети физических объектов с другими информационными системами; в) двунаправленность соединения (от/к физическому объекту); г) более широкие «интеллектуальные» возможности оконечных устройств; д) мультиплатформенность.

С этой точки зрения интернет вещей начинается там, где частные изолированные сети физических объектов, функционирующие со значительным вовлечением человеческих ресурсов, трансформируются в открытые экосистемы сервисов, которые ориентированы на дистанционную передачу данных от оконечных устройств, их анализ в режиме реального времени и телеуправление для оптимизации работы различных систем и ресурсов.

Оба подхода имеют право на жизнь.

Рис. 2. Эволюция инфраструктуры для интернета вещей

Границы рынка между традиционными системами автоматизации и решениями интернета вещей размыты.

При оценке объема рынка будем исходить из первого подхода: учитываются все решения, которые позволяют объединять «вещи» в сеть, даже если эти сети изолированные. Основная причина использования такого подхода – размытость границ между традиционными системами автоматизации и «чистыми» решениями интернета вещей, которые пока не представляется возможным как-либо выделить.

Объем рынка интернета вещей можно оценивать двумя способами:

1) по расходам потребителей на решения либо сервисы интернета вещей;

2) по выручке поставщиков IoT-решений от их внедрения.

Таблица 1. Задачи, решаемые с помощью систем интернета вещей на транспорте

Группа ИТС	Сервисы для пользователей ИТС
Управление дорожным движением	Поддержка транспортного планирования Управление дорожным движением Управление в чрезвычайных транспортных ситуациях Управление требованиями по транспортировке Политика в области регулирования дорожного движения Управление технической эксплуатацией инфраструктуры
Информация для пользователей транспорта	Информация перед поездкой Информация для водителей во время движения Информация для общественного транспорта во время движения Индивидуальные информационные услуги Дорожные руководства и навигация
Системы транспортных средств	Улучшение распознавания Автоматизированное управление Предупреждение лобовых столкновений Предупреждение боковых столкновений Системы безопасности Системы предотвращения аварий
Коммерческие транспортные средства	Предтаможенные операции на коммерческом транспорте Административные процессы на коммерческом транспорте Автоматизированная инспекция безопасности на дорогах Мониторинг безопасности в коммерческих автомобилях Управление парком коммерческих транспортных средств
Общественный транспорт	Управление общественным транспортом Управление транспортом по требованию Управление комбинированным транспортом
Управление в чрезвычайных ситуациях	Сигнализация об опасной ситуации и личная безопасность Управление аварийно-спасательным транспортом Опасные грузы и предупреждение инцидентов
Электронные платежи	Электронные финансовые перечисления
Безопасность	Безопасность в общественном транспорте Безопасность инвалидов Интеллектуальные перекрестки

Источник: PIARC, Ространспорт

Многоликий и многогранный

Интернет вещей – это следующий этап эволюции решений автоматизации бизнес-процессов с вовлечением физических объектов. Эволюция идет от аналоговой инфраструктуры сначала к цифровой, потом к адаптивной и позже к самоорганизующейся (рис. 2). Большинство бизнес-процессов в каждой отрасли уникально, а значит, уникальны и отраслевые IoT-решения. Поэтому рынок интернета вещей имеет ярко выраженную отраслевую специфику. Но и внутри отрасли присутствует множество разных технологических решений, которые решают разные бизнес-задачи конкретного потребителя. Например, есть разные типы транспорта – общественный наземный, железнодорожный пассажирский, легковой автотранспорт, коммерческий автомобильный грузовой и т.д. Каждый тип транспорта имеет свою специфику, которая учитывается в отраслевом решении. Более того, специфика информационной транспортной системы (ИТС) определяется также типом потребителя, на которого направлен сервис. Например, город решает задачи управления дорожным движением, пассажирам нужны сервисы навигации и информация о движении общественного транспорта, собственникам автопарка – возможности мониторинга и управления водителями и транспортными средствами и т.д. (табл. 1).

Такая же ситуация и в других отраслях экономики. В результате мир отраслевых решений интернета вещей очень многообразен. Поэтому при оценке и анализе спроса нужно отталкиваться от IoT-сервисов, которые предоставляются в конкретной сфере экономической деятельности определенным типом IoT-решений. Этот перечень уже достаточно внушителен и постоянно расширяется.

Вендорский vs потребительский

Чтобы предложить потребительский сервис, приходится разрабатывать комплексные решения, которые включают физические объекты («вещи»), сетевые компоненты и каналы связи для передачи данных от объектов, место для хранения этих данных и различные программные компоненты для собственно создания сервисов, нацеленных на конечных потребителей. На текущем эта-

Таблица 2.
Международные IoT-вендоры, которые присутствуют в России, но для которых IoT-бизнес не является основным

IoT-платформа	Компания	Происхождение	Основной бизнес
ABB Ability	ABB	Швейцария	Оборудование для энергетики
Bosch IoT Suite	Bosch SI	Германия	Бытовая техника
Predix	GE	США	Медицинское оборудование
Lumada	Hitachi	Япония	Электротехника, инструменты
Uniformance	Honeywell	США	Системы автоматизации
Watson IoT Platform	IBM	США	Программное обеспечение, компьютеры и устройства
Oracle IoT	Oracle	США	СУБД, программно-аппаратные комплексы
CityTouch	Signify (ранее Philips Lighting)	Нидерланды	Светодиодные и традиционные лампы
ThingWorx	PTC	США	Системы автоматизации
ARTIK Smart IoT Platform	Samsung	Южная Корея	Электронная техника
EcoStruxure	Schneider Electric	Франция	Оборудование для энергетики
Siemens Mindsphere	Siemens	Германия	Машиностроение

Источник: iKS-Consulting

пе технологического развития рынка велика роль системных интеграторов, которые «собирают» решения интернета вещей под конкретного заказчика, тиражируют его сначала в этой же отрасли, а потом – в смежных.

По данным IoT Analytics, глобальный вендорский IoT-рынок представлен более чем четырьмя сотнями IoT-платформ. Сегодня сформировались четыре основных сегмента IoT-платформ, различающиеся функциональными возможностями:

1. Платформы управления устройствами и IoT-шлюзы.
2. Платформы управления сетевой связностью.
3. Платформы управления данными.
4. Платформы управления приложениями.

Многие международные аналитические компании под термином «IoT-платформа» понимают только полнофункциональные платформы управления данными и приложениями. При этом следует понимать, что «IoT-платформа» – термин зачастую в значительной степени маркетинговый, который используется для позиционирования продукта. Оценить функциональные и технические возможности решения можно только путем детального анализа его технической документации. Нужно также учитывать, что IoT-платформы постоянно развиваются, дополняются и дорабатываются.

По критерию «сфера применения/отраслевая специализация» выделяют две основные группы IoT-платформ:

1. Полнофункциональные (или горизонтальные), например, PTC ThingWorx, Hitachi Lumada, Software AG Cumulocity IoT, Rightech IoT Cloud.
2. Специализированные вертикальные (отраслевые), например, Unilight от ГК «АйТи», GE Predix, EcoStruxure Schneider Electric.

На российском рынке присутствуют несколько десятков вендоров IoT-платформ, большая часть из которых – международные компании. Для многих из них IoT-бизнес является новым развивающимся направлением, и лишь некоторые уже имеют и реализуют локальные IoT-стратегии при наличии глобальных центров компетенций и коммерческих представительств в России. Практически все инвестируют и время, и финансовые средства в продвижение собственных IoT-разработок и евангелизацию технологий интернета вещей. Основная причина низкой активности международных IoT-вендоров на российском рынке – приоритизация географических рынков для развития по критерию «потенциал – простота реализации» не в пользу России.

Существуют разные сценарии внедрения IoT-решений:

- внедрение на крупном предприятии;
- внедрение на среднем/малом предприятии (как правило, при разработке собственных IoT-сервисов);
- использование IoT-платформы производителем оборудования и оконечных устройств;
- внедрение IoT-платформы для разработки и предоставления различных коробочных IoT-сервисов для вертикальных рынков.

Большинство реализованных кейсов в области IoT в России – это штучные комплексные проекты, реализуемые для крупных заказчиков при активном участии системных интеграторов.

В зависимости от реализуемого сценария различаются и технические стратегии внедрения. Эти различия определяются:

- степенью самостоятельности заказчика/участием во внедрении системного интегратора (как правило, большие сложные проекты требуют отраслевых и технологических компетенций);
- степенью интеграции IoT-платформы с существующими корпоративными информационными системами (биллинг, CRM, личные кабинеты заказчиков и пр.);
- потребностью в преднастроенных инструментах (для автоматизации биллинга, визуализации, анализа данных, разработки собственного брендированного пользовательского интерфейса и т.д.);
- объемами капитальных либо операционных затрат.

В России за последние несколько лет IoT-платформы внедрялись в основном на крупных предприятиях. Как правило, это вертикальные решения, нередко созданные в партнерстве с международными компаниями.

Например, Softline на платформе Microsoft Azure IoT разработала для компании «Криогенмаш» IoT-сервис удаленного мониторинга работы воздухоразделительной установки и сбора данных с определенным набором метрик для последующей разработки математической модели оптимизации процесса технического обслуживания и ремонта оборудования и ряда сопряженных бизнес-процессов (управление закупками, поставками, взаимоотношениями с поставщиками, финансовое и производственное планирование).

Philips Lighting сотрудничает с компанией «АйТи Энергофинанс» с целью создания комплексной интегрированной системы управления освещением на базе платформы Unilight.

В 2017 г. было много объявлений о намерениях и стратегических планах. Так, «Роснефть» (через дочернюю компанию ИК «Сибинтек») и General Electric подписали акционерное соглашение о создании совместного предприятия для развития в России промышленного интернета и внедрения передовых цифровых решений на объектах «Роснефти» и в российской нефтегазовой отрасли.

ГК «Ренова» объявила о создании компании «Цифра», которая будет разрабатывать собственные продукты, развивать существующие решения группы и вкладывать средства в перспективные технологии промышленного интернета и искусственного интеллекта в России и за рубежом. «Цифра» инвестировала в IIoT-систему мониторинга промышленного оборудования «Диспетчер», разработанную смоленской компанией ИЦ «Станкосервис». В рамках заключенной сделки объем капиталовложений до конца 2019 г. составит 850 млн руб.

Газпромбанк, «Мегафон», «Ростех» и USM Group организовали совместное предприятие «МФ Технологии», которое будет развивать проекты в сфере цифровой экономики, блокчейна и IoT.

Не остаются в стороне и другие операторы связи, которые активно наращивают свои возможности в сфере интернета вещей, в том числе через развертывание IoT-платформ, позволяющих создавать и предоставлять клиентам собственные IoT-сервисы. «Билайн» запускает свои сервисы на платформе Cisco Jasper. МТС тестирует решения на базе платформы Nokia Impact, уже упомянутый «Мегафон» – на платформе «Петер-Сервис» (летом 2018 г. «Мегафон» проводил закрытый конкурс на выбор новой полнофункциональной IoT-платформы). «ЭР-Телеком» строит свою IoT-сеть на базе платформы управления сетевой связностью Actility. Практически все операторы имеют в продуктовом портфеле свой набор IoT-сервисов.

Подводя итоги 2018 года

Очевидно, что при сохранении текущих темпов роста уходящий год не станет прорывным для российского рынка интернета вещей. Основной результат – создание в разных отраслях новых частных изолированных сетей физических объектов. Количество и качество таких частных сетей растет. Этому во многом способствуют IoT-вендоры, системные интеграторы и инжиниринговые компании.

Текущая рыночная конъюнктура сдерживает масштабные IoT-эксперименты и ограничивает количество долгосрочных проектов. Тем не менее разработка IoT-технологий продолжается, в том числе отечественными компаниями, среди которых Tibbo Systems, Rightech. В России создано много локальных отраслевых решений, например, в сфере ЖКХ – «Элдис», в сфере энергоэффективности – Unilight, на транспорте – «ЕвроМобайл», в промышленности – «Диспетчер». И этот список постоянно расширяется. Надо полагать, что с изменением экономической ситуации рынок заметно ускорит свое развитие. ИКС

Сертификация устойчивого развития: что, как и зачем

Интерес к «зеленым» стандартам строительства в России с каждым годом растет, увеличивается число проектов, успешно прошедших международную сертификацию. Какие выгоды дает такой сертификат?

Дмитрий Кузнецов, эксперт по системам автоматизации зданий и ЦОД, КРОК; консультант, DGNB

Интерес к сертификации устойчивого развития во многом обусловлен возведением большого количества спортивных объектов к событиям мирового масштаба: зимним Олимпийским играм в Сочи (2014 г.) и Чемпионату мира по футболу (2018 г.). И Международный олимпийский комитет, и ФИФА декларируют свою приверженность принципам устойчивого развития и транслируют соответствующие требования в регламентирующие документы по проектированию и строительству новых объектов. В частности, пять футбольных арен в Москве, Самаре, Нижнем Новгороде, Волгограде и Саранске прошли сертификацию проектной документации в соответствии с британским стандартом BREEAM (Building Research Establishment Environmental Assessment Method, метод оценки экологической эффективности зданий).

Однако если Европе и Америке концепция устойчивого развития давно близка и понятна, для России это пока новый аспект жизни общества. Давайте разберемся, как устойчивое развитие стало главным ориентиром деятельности в XXI веке, в чем особенности «зеленой» сертификации, какие она дает преимущества.

Быть в тренде

Устойчивое развитие определяется как развитие, при котором удовлетворение потребностей нынешних поколений осуществляется без ущерба для интересов будущих. Эта формулировка появилась в 1987 г. в докладе «Наше общее будущее», подготовленном Международной комиссией ООН по окружающей среде и развитию. Помимо этого, согласно концепции тройного критерия (triple bottom line), считается, что устойчивое развитие находится на пересечении трех его неотъемлемых компонентов: окружающей среды, экономики и социальной сферы (рис. 1).

На сегодняшний день концепция устойчивого развития стала общепризнанным мировым трендом, который в той или иной степени проявляется во всех сферах жизни: от бережной и ответственной заготовки древесины до принципов приема на работу. В строительной отрасли наиболее полное отражение концепция нашла в сертифицирующих системах – «зеленых» стандартах, впервые появившихся в Европе и Америке на рубеже XXI века. В большинстве своем такая сертификация носит рекомендательный характер, она оценивает объект на соответствие целому ряду экокритериев и по количеству набранных баллов присваивает ему тот или иной уровень экологичности и энергоэффективности.

Со временем национальные системы оценки появились во многих странах, однако международную известность и признание получили только три: британская BREEAM (1990 г.), американская LEED (Leadership in Energy and Environmental Design, Руководство по энергоэффективному и экологическому проектированию, 1998 г.) и немецкая DGNB (Deutsche Gesellschaft für Nachhaltiges Bauen, Немецкий совет по устойчивому строительству, 2009 г.). В настоящее время по ним уже сертифицировано более 600 тыс. объектов: по BREEAM – более 560 тыс., по LEED – более 49 тыс. и по DGNB – более 900.

В России «зеленые» стандарты начали приобретать популярность с 2010 г., когда были выданы первые сертификаты на коммерческие объекты. В 2014 г. по инициативе Российской гильдии управляющих и девелоперов на основе чет-

Рис. 1. Концепция тройного критерия

Рис. 2. **Динамика появления сертифицированных объектов в России**

По данным АНО «НИИУРС», июнь 2018

вертой версии системы LEED (LEED v.4, 2014) была создана отечественная система устойчивого развития в строительстве – Green ZOOM. Она адаптирована к нашим реалиям и учитывает требования российских нормативно-технических документов. На сегодняшний день по ней сертифицировано свыше 30 объектов в разных секторах недвижимости (рис. 2).

Главное – правильное начало

В каждой «зеленой» системе есть свои особенности, но в целом их принципы схожи. Рассмотрим процесс прохождения сертификации на примере систем LEED и DGNB, только набирающих популярность в России и потому не так часто встречающихся в обзорных материалах.

Во-первых, необходимо выбрать схему сертификации, которая позволяет учесть специфику объекта. Требования, например, к отелям и складским зданиям ощутимо различаются. В немецкой системе DGNB таких схем девять: офисы, образовательные учреждения, жилье, отели, три разновидности торговых объектов и две разновидности промышленных зданий. Для объектов смешанного использования существует отдельная схема.

В американской системе LEED классификация сложнее. Всего можно выделить четыре большие группы со специфическими схемами внутри них: новое проектирование и строительство (LEED for Building Design and Construction), интерьерный дизайн (LEED for Interior Design and Construction), существующие здания (LEED for Building Operations and Maintenance) и развитие территорий (LEED for Neighborhood Development). Отмечу, что в LEED нет возможности оценить здание смешанного использования. Для таких случаев действует правило 40/60: если несколько схем подходят для 40–60% общей площади объекта, то решение о ее выборе принимается проектной командой вместе с заказчиком.

Следующий шаг – выбор стадийности проведения сертификации. Обе системы позволяют как выполнить ее в один этап и сразу получить оценку готового объекта, так и разделить ее на пресертификацию на этапе проектирования и завершение сертификации после окончания строительства. Такая возможность разделения на этапы полезна в случае длительного перерыва между проектированием и строительством, а также в качестве аудита проектных решений. За-

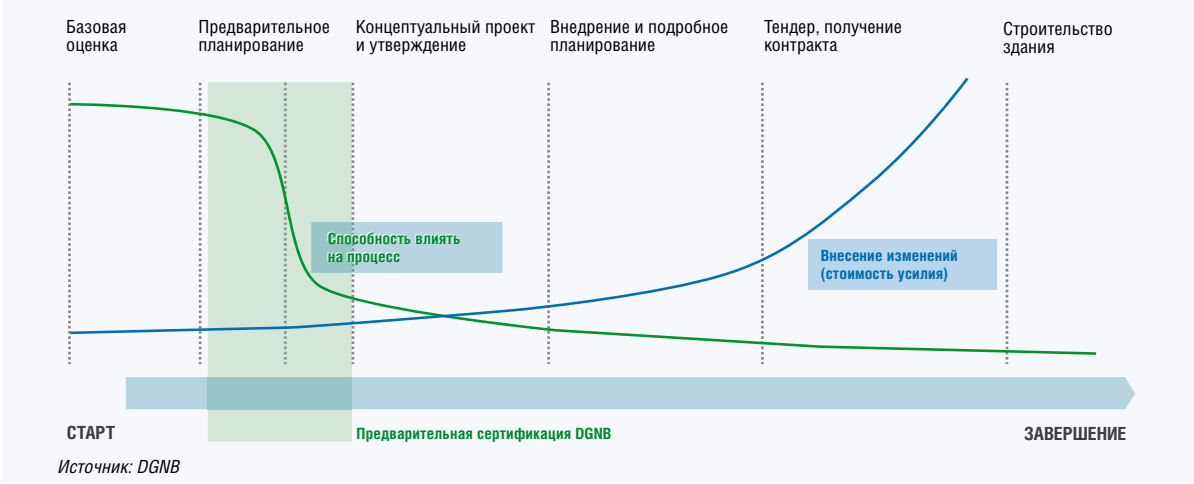


Рис. 3. **Возможность и стоимость внесения изменений в проект на разных этапах жизненного цикла**

Источник: DGNB

казчик может уже на этой стадии выяснить, на какой уровень сертификата рассчитывать, и при необходимости внести изменения в проект. Естественно, стоимость корректировки решений в самом начале жизненного цикла объекта значительно меньше, чем на последующих этапах (рис. 3).

Соответствие стандартам

После выбора схемы и стадийности сертификации начинается основной этап – проверка соответствия параметров объекта критериям «зеленого» стандарта.

В системе LEED таких критериев 57 (могут различаться в зависимости от схемы сертификации). Они сгруппированы в девять разделов, описывающих требования к объекту с различных позиций принципа тройного критерия:

- интегрированный процесс (Integrative Process, IP);
- местоположение и транспортная инфраструктура (Location and Transportation, LT);
- устойчивое развитие территории (Sustainable Sites, SS);
- эффективность водопотребления (Water Efficiency, WE);
- энергоэффективность и выбросы в атмосферу (Energy and Atmosphere, EA);
- использование материалов и ресурсов (Materials and Resources, MR);
- качество среды внутри помещений (Indoor Environmental Quality, IEQ);
- инновации в проектировании (Innovation in Design, ID);
- региональные особенности (Regional Priority, RP).

Оценка по некоторым критериям обязательна, иначе сертификация объекта невозможна. Например, в случае LEED BD + C это целый ряд параметров, которые отслеживают предотвращение загрязнения окружающей среды в процессе строительства, управление строительным мусором и отходами, идущими на переработку, уменьшение использования воды, электроэнергии, минимальные требования к качеству внутренней среды. Важность остальных критериев определяется присуждаемым за них количеством баллов. Так, самый приоритетный критерий в LEED BD + C – возможность оптимизации энергопотребления – оценивается в 18 баллов, а системы учета потребления воды и электроэнергии – всего лишь по 1 баллу.

По сумме баллов определяется уровень сертификата: больше 80 баллов – «платина» (LEED Platinum), 60–79 баллов – «золото» (LEED Gold), 50–59 баллов – «серебро» (LEED Silver), 40–49 баллов – «бронза», или просто статус «сертифицировано» (LEED Certified).

Система DGNB содержит 37 критериев, разделенных на шесть групп:

- качество окружающей среды (Environmental Quality);
- экономическая эффективность (Economic Quality);
- социально-культурные качества и функциональность (Socio-Cultural and Functional Quality);
- техническая оснащенность (Technical Quality);
- качество процессов планирования и строительства (Process Quality);
- качество месторасположения (Site Quality).

Максимальная оценка по каждому из критериев – 100, также можно получить определенное количество бонусов. Однако итоговый результат складывается не просто из суммы баллов, учитывается важность (вес) критерия. Например, в схеме сертификации офисов самыми важными являются критерий ENV1.1 «Оценка жизненного цикла здания» (фактор важности – 8, вклад в общую оценку – 9,5%), критерий ECO1.1 «Стоимость жизненного цикла» (фактор – 4, вклад – 10%) и критерий ECO2.1 «Гибкость и адаптация» (фактор – 3, вклад – 7,5%). Наименее важные критерии – ENV2.4 «Биоразнообразие на территории» (фактор – 1, вклад – 1,2%) и SOC1.7 «Безопасность и охрана» (фактор – 1, вклад – 1%).

Помимо важности каждого критерия в отдельности, в DGNB учитывается вес каждой группы. Это сделано для того, чтобы при оценке объекта его вклад и влияние на окружающую среду значили не меньше, чем, например, экономические показатели.

После оценки объекта по всем критериям по определенной математической формуле вычисляется итоговый индекс эффективности. По нему, а также по индексу каждой отдельной группы (кроме качества территории, которая чаще всего является просто исходными данными) определяется уровень сертификата – «бронза» (или статус «сертифицировано»), «серебро», «золото» или «платина». Таким образом, для получения, скажем, золотого уровня недостаточно, чтобы итоговый индекс был больше 65%, необходимо по каждой из пяти групп критериев набрать не менее 50% (рис. 4).

Помощь в прохождении

Процесс прохождения сертификации также имеет свои особенности в зависимости от выбранной системы.

Для сопровождения процесса сертификации по LEED формируется команда, в задачи которой входят: регистрация проекта в базе данных USGBC (U.S. Green Building Council, Амери-

Рис. 4. Уровни сертификации в системе DGNB

Итоговый индекс	Минимальный индекс	Уровень сертификата
от 35%	—	Бронза *
от 50%	35%	Серебро
от 65%	50%	Золото
от 80%	65%	Платина

* Только для построенных зданий

Источник: DGNB

канский совет по зеленому строительству), оценка объекта по списку критериев, подготовка подтверждающих документов, общение с заказчиком, проектировщиками и строителями, с одной стороны, и с представителями сертифицирующего органа – с другой. Никаких жестких требований к квалификации команды нет – это могут быть как представители генпроектировщика, генподрядчика или собственные специалисты заказчика/инвестора, так и эксперты компании, предоставляющей услуги по сертификации объектов. Например, в одном из проектов КРОК выступал консультантом в сфере энергоэффективности и экологичности зданий: наши специалисты подбирали материалы и оборудование, разрабатывали оптимальные решения в инженерной и ИТ-областях. В результате объект получил сертификат LEED уровня Gold.

В XXI веке концепция устойчивого развития постепенно становится новой философией бизнеса. Поэтому в системе LEED есть возможность пройти специализированное обучение (с последующей сдачей экзаменов и получением сертификата), посвященное как этой области в целом, так и конкретным схемам сертификации и процессу их прохождения. Выделяются два уровня квалификации – ассоциированный член (Green Associate) и аккредитованный специалист (Accredited Professional). Если при прохождении сертификации в проектной команде есть хотя бы один LEED AP, то это дает дополнительный балл в разделе «Инновации».

Главное отличие системы DGNB в том, что сертификация объекта в обязательном порядке выполняется аккредитованным аудитором, с которым заключается отдельный договор. В этом случае не проектная команда, а отдельный человек отвечает за прохождение этапов сертификации и все коммуникации в ее процессе.

В DGNB также есть несколько ступеней обучения, но именно для специалистов, выполняющих сертификацию, – зарегистрированный профессионал (Registered Professional), консультант (Consultant) и аудитор (Auditor). Причем переход на последний уровень для консультанта становится возможным только после самостоятельной сертификации объекта. Список всех специалистов второй и третьей ступени доступен на сайте Немецкого совета по устойчивому строительству. Сегодня в России, например, 26 консультантов и шесть аудиторов.

В остальном процессы прохождения сертификации совпадают. Инвестор или владелец объекта видит необходимость по завершении строительства получить сертификат системы устойчивого развития. Заключается договор с компанией-аудитором, которая будет выступать независимой стороной процесса проектирования и строительства и возьмет на себя проведение сертификации. Все технические решения принимаются при постоянном трехстороннем взаимодействии аудитора, заказчика и проектировщика (или строителя). Здесь важна именно эффективная коммуникация участников.

Например, заказчик видит свои ограничения бюджета. Проектировщик/строитель – совокупную стоимость строительства. Аудитор понимает, как те или иные решения повлияют на возможную оценку, и исходя из этого оценивает их, предлагает внести изменения в проект. Кроме того, он может спрогнозировать, как корректировки повлияют на стоимость эксплуатации и обслуживания и, следовательно, на полную стоимость владения объектом. В системе DGNB это позволяет сделать один из критериев – «Стоимость жизненного цикла» ECO1.1. Благодаря этому уже на этапе проектирования можно сравнить несколько вариантов реализации.

Цена вопроса

Стоимость сертификации объекта нужно разделить на две составляющие. Первая и, как правило, большая часть – добавленная стоимость архитектурных, строительных и инженерных решений, реализация которых позволит получить сертификат необходимого уровня. Вторая – стоимость самой сертификации. Эта сумма также состоит из нескольких частей – фиксированной и переменной.

Фиксированная часть – плата сертифицирующему органу. В случае LEED – Американскому совету по зеленому строительству; в случае DGNB – Немецкому совету по устойчивому строительству. Размер платы зависит от общей площади объекта, выбранной схемы, стадийности сертификации и членства клиента в данных ор-

ганизациях. Например, для нового офисного здания общей площадью 10 тыс. кв. м при условии, что клиент не является членом вышеупомянутых советов, стоимость одностадийной сертификации составит:

1. Для LEED:
- регистрация проекта – $1500;
- плата в зависимости от площади (108 тыс. кв. футов), округленно – $7320;
- итого – $8820.

2. Для DGNB:
- плата в зависимости от площади (7500–10 000 кв. м) – €11 100;
- 20% стоимости платится при регистрации проекта, 20% – за пресертификацию (проект), оставшаяся часть – за финальный сертификат.

Переменная часть стоимости – это плата конкретной компании или аудитору за помощь в прохождении сертификации. Она может зависеть также от количества вариантов проекта, которые заказчик хочет оценить на предмет общей стоимости жизненного цикла. Размер этой составляющей сложно назвать априори, поскольку она уникальна для каждого объекта, т.е. напрямую зависит от желаемого уровня сертификата и выбранных архитектурных и инженерных решений. Согласно отчету компании Drees & Sommer, стоимость дополнительных проектных и консультационных услуг по системе DGNB составляет меньше 0,5% общей стоимости строительства. Дополнительные строительные расходы могут варьироваться от 0 до 4% для DGNB и до 7% для LEED.

Зачем сертифицировать

В России основной стимул сертификации коммерческой недвижимости – маркетинг. Факт ее успешного прохождения подтверждает статус и престижность объекта, что помогает привлечь клиентов и увеличить ставку арендной платы по сравнению с несертифицированными зданиями.

Для некоторых, в основном иностранных, арендаторов наличие «зеленого» сертификата является обязательным при выборе офисных площадей. Такой сертификат подтверждает, во-первых, что данная недвижимость спроектирована и построена с соблюдением принципов экологической и социальной ответственности и соответствует общемировому тренду устойчивого развития. Во-вторых, он говорит об энергоэффективности здания, а значит, меньших расходах на оплату потребляемой энергии.

Однако высокая маркетинговая привлекательность объекта – только вершина айсберга. Сам принцип устойчивого развития подразумевает, что все участники процесса заинтересованы в следовании требованиям экологического, социального и экономического критериев и вознаграждаются соответственно. В случае рассматриваемых систем сертификации задействованные стороны – это конечные пользователи (например, арендаторы), владельцы или инвесторы, архитекторы, проектировщики, строители и эксплуатирующие службы, производители оборудования и строительных материалов, консультанты и аудиторы. И каждая из этих групп получает свою выгоду:
- пользователи – более высокое качество жизни за счет здоровой среды в здании, уменьшения расходов на оплату потребляемых ресурсов, а также благодаря более бережному отношению к окружающей среде в целом;
- владельцы и инвесторы – оптимальное решение с меньшими рисками и расходами на эксплуатацию, более высокой привлекательностью для клиентов и кредитных организаций, повышение деловой репутации на национальном и мировом уровне;
- участники проектного и строительного процесса – меньшие финансовые и временные затраты на достижение согласованного результата, продвижение принципов интегрированного процесса проектирования и строительства, понятные и прозрачные требования к конечному продукту;
- производители – четкие требования к продукции и возможность адекватного планирования развития и вложения средств в модернизацию или расширение производства;
- консультанты – возможность продвижения передовых технологий в проектировании и строительстве, например BIM-технологии, и интегрированный и четко регламентированный процесс пусконаладки и передачи объекта в эксплуатацию (commissioning).

Помимо этого, список критериев каждой из систем сертификации можно рассматривать как своеобразный опросный лист или технические требования для любого проекта, даже если нет цели получить сертификат. В целом стандарты устойчивого развития задают ориентир и понимание того, каковы на текущий момент лучшие практики в области гражданского проектирования и строительства. Таким образом, сертификация – это сильный технический, экспертный и аудиторский инструмент, продвигающий инновационные подходы и технологии, которые позволяют получить наилучший результат при снижении любых видов затрат. ИКС

Правовой риск-менеджмент в дата-центре

Сергей Смолин, заместитель руководителя юридического департамента, DataSpace

Надежного оператора ЦОДа отличает тщательно проработанный и организованный риск-менеджмент, способствующий надежной и бесперебойной работе дата-центра.

Чем выше заявленный уровень надежности и отказоустойчивости дата-центра, тем больше ответственности должен брать на себя его оператор и тем тщательнее подходить к риск-менеджменту, поскольку материализация рисков может нанести значительный ущерб и ему самому, и его клиентам. В отличие от правового риск-менеджмента прочей недвижимости, такой как складские или офисные помещения, правовой риск-менеджмент ЦОДа во многом связан с обеспечением возможности круглосуточного функционирования этого объекта и с защитой интересов его клиентов.

Список правовых рисков, с которыми сталкивается оператор ЦОДа, открыт: в любой момент могут возникнуть новые факторы, влияющие на функционирование дата-центра. Поэтому от оператора ЦОДа требуется грамотный подход к управлению рисками, а также к формированию принципов и процессов управления и систематизации потенциальных рисков. Рассмотрим основные группы правовых рисков, которые должен учитывать оператор ЦОДа.

Риски нарушения законодательства

Процесс управления дата-центром должен соответствовать требованиям законодательства РФ. Таких требований достаточно много, начиная от правил охраны труда до норм выброса загрязняющих веществ в атмосферу. Правовой риск-менеджмент в данной области направлен как на оценку новых рисков, так и на предотвращение материализации уже известных. Законодательство часто меняется, и оператор ЦОДа должен постоянно следить за актуальными нормативными актами и правоприменительной практикой, составлять регламенты и методические рекомендации для сотрудников и т.д. В случае изменения законодательства он обязан оперативно адаптировать дата-центр под новые требования. Нарушение законодательства недопустимо, поэтому регулярный правовой аудит всех процедур дата-центра – первостепенная задача.

Кроме того, всегда существует риск неумышленного нарушения законодательства или совершения административного правонарушения. В такой ситуации юридическая служба оператора ЦОДа должна обеспечить надежную правовую защиту интересов компании и ее сотрудников, а также исключить возможность влияния санкций контролирующих органов на качество услуг, оказываемых дата-центром.

Риски в договорных правоотношениях

При взаимодействии с клиентами, подрядчиками или поставщиками оператор ЦОДа может столкнуться со многими правовыми рисками. Это могут быть риски задержки оплаты услуг клиентом либо риски неисполнения или ненадлежащего исполнения контрагентами своих обязательств, например, поставки неисправного оборудования. Возможны непредвиденные ситуации (скажем, поставщик не может предоставить заказанное оборудование, поскольку его производство прекращено), либо наступление событий, не зависящих от воли ни одной из сторон (форс-мажор), в частности, стихийных бедствий.

Во всех вышеперечисленных ситуациях грамотный правовой риск-менеджмент обеспечивает оператору ЦОДа надежную защиту. Некоторые риски можно минимизировать тщательной проработкой договора, в котором нужно предусмотреть способ урегулирования спорных ситуаций. Для рисков, связанных с непредвиденными ситуациями, оператор ЦОДа должен прибегать к резервированию поставок или услуг: например, если бесперебойное электропитание дата-центра обеспечивается дизель-генераторными установками, необходимо иметь контракты с несколькими поставщиками топлива, чтобы в случае невозможности получения топлива от одного поставщика другой мог его заменить.

Участие оператора ЦОДа в судебных разбирательствах

Причин, по которым оператор ЦОДа может быть вовлечен в судебные разбирательства, множество: заставить его обратиться в суд могут, например, задолженность со стороны клиента или недопоставка оборудования поставщиком. Судебный

процесс отнимает много времени и ресурсов. Правовой риск-менеджмент в этой сфере, как правило, направлен на досудебное урегулирование споров, а риск-менеджмент в области договорных правоотношений помогает обеспечить для такого урегулирования комфортные условия.

Также есть риск, что оператор ЦОДа окажется вовлечен в судебный спор в качестве ответчика. Причиной может стать неисполнение каких-либо взятых на себя обязательств. Участие в таких судебных процессах может нанести оператору ЦОДа как имущественный, так и репутационный ущерб. Грамотный риск-менеджмент в данной ситуации должен обеспечить формирование надежной правовой позиции оператора ЦОДа, а также исключить влияние судебного спора на качество услуг дата-центра.

Риски управления недвижимостью

Количество рисков, связанных с управлением зданием дата-центра, зависит от того, является оператор ЦОДа собственником или арендатором здания и земельного участка. В последнем случае рисков намного больше. Но в обоих случаях правовой риск-менеджмент направлен на то, чтобы исключить возможность потери оператором контроля над дата-центром.

Если оператор ЦОДа – арендатор здания, то в первую очередь необходимо исключить риск прекращения аренды по инициативе собственника здания. Этого можно добиться, заключив долгосрочный договор аренды, но и это полностью не устраняет риска потери контроля над дата-центром: собственник может продать здание либо обанкротиться и т.п. Для услуг colocation большое значение имеет гарантированное право на владение дата-центром. Такой гарантией может стать зафиксированное в договоре аренды преимущественное право выкупа здания оператором ЦОДа.

Если же оператор ЦОДа является собственником здания и земельного участка, то объем его правовых рисков значительно меньше. Тем не менее он должен обеспечить надежную правовую защиту активов от возможных имущественных требований третьих лиц или противозаконных действий, направленных на лишение оператора ЦОДа его имущества. В данной ситуации правовой риск-менеджмент заключается в создании грамотной структуры владения имуществом, его страховании и правовой защите.

Еще один риск связан с проектированием и строительством ЦОДа. В процессе строительства могут возникнуть разнообразные правовые риски, многие из которых критичны для дальнейшего функционирования дата-центра. Например, земельный участок под ЦОД является предметом спора в суде, собственник соседнего земельного участка ограничивает доступ к дата-центру, изменение категории земельного участка накладывает ограничение на его использование – все эти риски можно предвидеть и устранить при грамотном подходе к правовому анализу объекта строительства. Квалифицированный due diligence на всех этапах возведения дата-центра гарантирует оператору ЦОДа надежную правовую защиту.

Внутрикорпоративные риски

Для качественного оказания услуг дата-центра большое значение имеют грамотно выстроенная корпоративная структура оператора ЦОДа и правильно подобранный и обученный персонал. Понятно, что конфликты между акционерами ЦОДа могут нанести значительный ущерб качеству оказываемых услуг и отразиться на клиентах дата-центра. Правовой риск-менеджмент должен быть направлен на минимизацию влияния споров акционеров ЦОДа на его функционирование. Этой цели должна служить тщательная проработка уставных документов, акционерных отношений и т.д.

В процессе оказания услуг дата-центра важную роль играет его персонал. Поэтому в ЦОДе так важна продуманная кадровая политика. Недопустимо, чтобы ответственные сотрудники не имели требуемого уровня квалификации или не прошли необходимое обучение.

Регулярный мониторинг изменений в законодательстве, оценка правового и финансового состояния контрагентов, продуманная кадровая политика – вот слагаемые качественного правового риск-менеджмента ЦОДа, повышающего надежность оказания его услуг.

Цель правового риск-менеджмента дата-центра заключается в том, чтобы предвидеть все вероятные риски и устранить их. Поэтому он должен не ограничиваться контролем за существующими рисками, но включать оценку любых новых рисков для дата-центра. Для этого в юридическом департаменте ЦОДа должна работать команда опытных специалистов. В противном случае дата-центр может оказаться не готовым к материализации того или иного риска. Если оператор не уверен в том, что все возможные риски для управляемого им дата-центра проанализированы, необходимо обратиться за помощью к компаниям, осуществляющим аудит дата-центров, в том числе юридический. ИКС

Оптимизация для цифровой трансформации

Александра Крылова

Без инженерной инфраструктуры не бывает ЦОДов, а они, как известно, фундамент цифровой экономики. Неудивительно, что вендоры, поставляющие решения для таких объектов, вносят изменения в свои концепции и продуктовые линейки с прицелом на цифровизацию.

Свои продукты и решения, позволяющие оптимизировать работу дата-центров сегодня и без потерь войти в эпоху цифровой экономики, ведущие зарубежные и российские производители представили на 13-й международной конференции «ЦОД-2018», организованной «ИКС-Медиа».

Из «одних рук»

Инженерная инфраструктура – это совокупность систем, каждая из которых работает на обеспечение отказоустойчивой работы ИТ-систем и сервисов. Гарантировать совместимость и интеграцию всех подсистем, а также их корректное взаимодействие на этапе эксплуатации помогает использование оборудования «из одних рук», считает Алексей Волков, менеджер по работе с партнерами Tripp Manufacturing Company, американского производителя систем защиты электропитания с 80-летней историей. Ставка на комплексность – принципиальная позиция вендора. В его продуктовом портфеле – электротехническое оборудование, кабельная продукция, конструктивы и ПО, необходимые для организации системы гарантированного бесперебойного электропитания в ЦОДе. Под торговой маркой Tripp Lite он выпускает, в частности, трехфазные ИБП мощностью от 10 до 400 кВА с коэффициентом мощности 0,9–1, блоки распределения питания, среди которых есть устройства базового уровня, а также измерительные и дистанционно управляемые БРП.

Системы защиты питания вписываются в напольные шкафы и открытые стойки серии SMARTRACK, предназначенные для ИТ- и телеком-оборудования. Все эти конструктивы поддерживают размещение оборудования с высокой плотностью. Их отличает высокая несущая способность – до 1360 кг, а площадь перфорации дверей у них больше, чем этого требуют производители серверов. Контроль за состоянием ИБП и сетевых блоков распределения питания обеспечивает бесплатное ПО Power Alert Network Management System, способное собирать по SNMP-протоколу данные с 250 разных устройств.

Весь спектр продуктов и услуг от концептуальной модели до сервисного обслуживания «из одних рук» предлагает компания Rittal. Немецкий производитель сфокусировал свою продуктовую стратегию на дата-центрах, поддерживающих граничные вычисления, которых по мере перехода экономики на цифровые рельсы будет требоваться все больше.

Фокусными для новой стратегии стали гибкость, стандартизируемость и масштабируемость инженерной инфраструктуры – свойства, приобретающие все большую ценность в глазах заказчиков Edge-ЦОДов. Для периферийных дата-центров в портфеле Rittal есть широкий спектр законченных решений – от микроЦОДов до преднастроенных и протестированных в фабричных условиях модульных и контейнерных решений.

Впрочем, при построении ЦОДов любого масштаба спрос на стандартизованные решения для всех инженерных задач будет расти: ведь стандартизация – это залог быстрого масштабирования. А кроме того, как заметил Кирилл Дмитриев, менеджер по продукции (ИТ-охлаждение) компании Rittal, благодаря ей можно подобрать лучшее решение для любой отрасли.

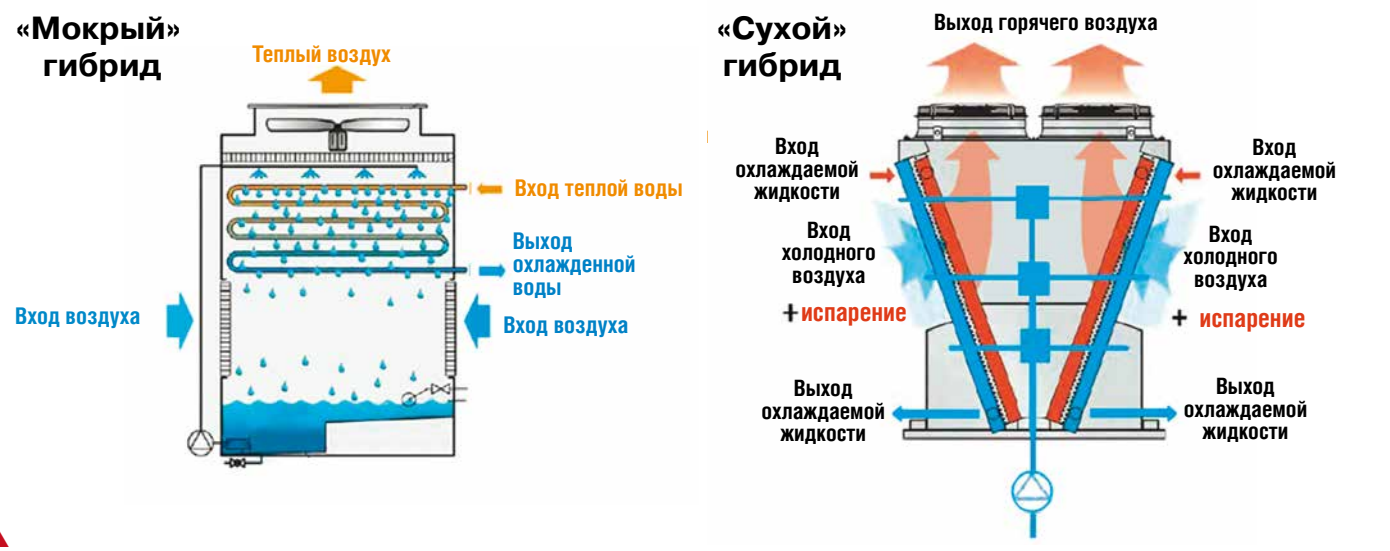
Так, для «умных» больниц и поликлиник, которым критически важна высоконадежная защита персональных медицинских данных пациентов, подойдет микроЦОД, в корпус которого заключена вся инженерная инфраструктура. Задачам операторов связи, которые готовятся к развертыванию сетей 5G, вполне соответствуют prefabricated-решения в формате модуля или контейнера. А кредитным организациям, пристально наблюдающим за обработкой платежных транзакций, стоит остановиться на другом преднастроенном на заводе Rittal решении – «ЦОДе из коробки», обеспечивающем к тому же мониторинг всех процессов.

ИБП с проверенными и новыми возможностями

Продукция мирового поставщика решений в области безопасного и устойчивого управления энергией, KEHUA Tech, известного как в Китае, так и за его пределами, стала доступна и российским цодостроителям с подачи его официального поставщика в России компании «Абитех».

Источники бесперебойного питания KEHUA производит на базе компонентов собственной разработки, и это наряду с системой контроля качества на всех этапах положительно сказывается

ДКС выпускает модернизированные шкафы для ИТ-оборудования



Гибридные аппараты на основе испарительных и «сухих» градирен

на надежности однофазных и трехфазных ИБП, трансформаторных и бестрансформаторных.

Для ЦОДов у KEHUA есть несколько серий такого оборудования. Серия KEHUA KR 33 объединяет системы защиты электропитания мощностью от 10 до 200 кВА с КПД 95%. Благодаря модульной архитектуре их ремонт сводится к замене неисправного модуля новым в «горячем» режиме.

Более мощные ИБП (25–600 кВА) серии KEHUA MR 33 отличает особая гибкость. Для построения этих систем могут использоваться три типа силовых модулей мощностью 25, 40 или 50 кВА и пять конструктивов шкафов. На плановый КПД – 96% – эти источники выходят уже при 10%-ной нагрузке. Достижению такого показателя способствует и наличие функции «спящего» режима, в который могут переходить ненагруженные силовые модули.

Повышенной надежностью отличаются ИБП KEHUA серии FR-UK с однофазным или трехфазным выходом, которые производитель позиционирует как системы защиты питания в промышленности. Для обеспечения надежности в конструкции этих модульных трансформаторных ИБП предусмотрены электромагнитное экранирование основной управляющей платы, два воздуховода для защиты от перегрева ключевых компонентов, функция управления синхронизацией с двойной шиной и замена вентиляторов в режиме онлайн. В портфеле вендора есть также трехфазные ИБП с литий-ионными батареями.

Число поставщиков систем защиты электропитания с батареями этого типа увеличивается. Не так давно их ряды пополнила компания Vertiv – так с конца 2016 г. называется подразделение Network Power корпорации Emerson, перешедшее в собственность компании Platinum Equity. В качестве поставщиков литий-ионных элементов питания Vertiv выбрала Samsung SDI и LG Chem. По словам Евгения Журавлева, руководителя направления продаж ИБП и модульных ЦОДов представительства Vertiv в России и Белоруссии, системы с литий-ионными батареями все более востребованы заказчиками, в том числе и потому, что во все такие АКБ обязательно встраиваются системы управления и мониторинга.

Также за время, прошедшее после смены собственника, компания Vertiv обновила продуктовую линейку моноблочных систем и модульных ИБП под брендом Liebert. После вывода на рынок модульной системы Liebert APM 600 с двойным преобразованием, предназначенной для защиты критически важных систем и обладающей децентрализованной архитектурой, компания «закрывает» весь спектр запросов заказчиков. Номинальная мощность Liebert APM 600 – от 50 до 400/600 кВА (с шагом 50 кВА), КПД в режиме VFI (voltage frequency independent), при котором система питает нагрузку напряжением, полностью стабилизированным по частоте и амплитуде, – 96,3%, выходной коэффициент мощности равен 1. ИБП совместим как с индуктивной, так и с емкостной нагрузкой, поддерживает параллельное подключение двух устройств.

Помимо линейки источников бесперебойного питания, компания Vertiv обновила и линейку стандартизированных решений для Edge-ЦОДов – All-in-one. Сегодня в ней есть микроЦОД EDGE Solution Small Size в формфакторе ИТ-шкафа, укомплектованный всеми системами жизнеобеспечения дата-центра, и типовые контейнерные решения – EDGE Solution Medium Size.

Больше надежности и эффективности

Компания ДКС, которая позиционирует себя как лидер российского электротехнического рынка, поставляет в центры обработки данных около 20 видов продуктов, хорошо зарекомен-

довавших себя в крупных российских дата-центрах. Так, щитовое оборудование, кабеленесущие системы и молниезащита производства ДКС используются в ЦОДе «Авантаж» и в мега-ЦОДе Сбербанка в Сколково.

Производит вендор и напольные шкафы разного назначения – универсальные напольные, для распределения электроэнергии, а также для ИТ- и телеком-оборудования. Универсальные сборные напольные шкафы выполняются из листовой стали толщиной не менее 1,5 мм, соответствуют как международным, так и российским стандартам (IP-55, IP-65, IK10, УХЛ1 по ГОСТ 15150), выдерживают нагрузку в 1000 кг и совместимы с активным оборудованием ведущих мировых и отечественных производителей. Шкафы для распределения электроэнергии с максимальной силой тока до 6300 А устойчивы к току короткого замыкания 100 кА и отличаются степенью секционирования (4b), обеспечивающей отделение функциональных узлов друг от друга и от шин, что повышает безопасность обслуживающего персонала.

В этом году компания ДКС существенно модернизировала линейку ИТ- и телекоммуникационных шкафов. Теперь их производство осуществляется полностью роботизированной линией на универсальной пыле- и влагозащищенной платформе (от IP25 до IP55), что обеспечивает высокую степень стандартизации всех компонентов. В линейке представлены шкафы для ИТ- и телеком-оборудования высотой 24, 38, 42 и 47U, шириной 600 или 800 мм и глубиной 600, 800, 1000 и 1200 мм. Заказчикам на выбор предлагается дверь из тонированного закаленного стекла, перфорированная или сплошная дверь. Распределенная несущая способность каждого такого шкафа – 1500 кг.

В процессе цифровизации экономики, когда дата-центров требуется много, их владельцам важно оптимизировать операционные издержки на этапе эксплуатации. По данным компании CyberPower Systems, 50% всех случаев возникновения перебоев в работе ЦОДов имеют причиной неисправные (27%) и разряженные (23%) свинцово-кислотные или никель-кадмиевые ак-

Готовим почву для будущего

По данным агентства «Литвинчук маркетинг», в 2017 г. объем рынка промышленного холодильного и климатического оборудования в ЕАЭС составил 20–25 млрд руб., и потребности в таких системах продолжают расти. Для их удовлетворения ГК «ТЕРМОКУЛ» в январе 2018 г. начала в свободной экономической зоне на границе Московской и Калужской областей строительство завода «Рефкул» общей площадью 13 тыс. кв. м, из которых около 8,5 тыс. кв. м – производственные и складские помещения.

По словам Алексея Морозова, заместителя генерального директора ГК «ТЕРМОКУЛ», завод «Рефкул» позиционируется как OEM-производство, которое будет задействовано для выпуска оборудования «ТЕРМОКУЛ» (холодильных аппаратов мощностью до 3 МВт, моноблочных чиллеров мощностью 1,4–1,5 МВт, технологических установок мощностью до 12 МВт и презиционных кондиционеров 50–300 кВт). Также здесь будет изготавливаться HVACR-оборудование для отдельных российских производителей и нестандартные единицы климатического оборудования для ряда телекоммуникационных компаний. Кроме того, производственные линии «Рефкул» будут использоваться для локализации производства оборудования иностранных компаний. Первым заказчиком и партнером стала итальянская компания HiRef, разместившая на заводе, неофициальное открытие которого намечено на декабрь, партию из 50 презиционных кондиционеров шкафного типа мощностью 10–50 кВт. Ее выпуск начнется в январе 2019 г., а на второе полугодие запланирован старт производства межрядных кондиционеров HiRef. По словам А. Морозова, оборудование будет полностью сертифицировано по системе европейских стандартов.

Рынок климатического и холодильного оборудования РФ

кумуляторные батареи. Также нужно принимать во внимание, что примерно 5% батарей этих типов выходят из строя в течение гарантийного срока.

Для того чтобы быстро выявить в большом батарейном массиве деградирующую АКБ и своевременно ее заменить, компания CyberPower Systems предлагает свою систему управления батарейным комплексом (Batteries Management System). Она представляет собой совместимый с ИБП контроллер и набор датчиков. Датчики устанавливаются на каждую батарею и с заданной периодичностью передают контроллеру информацию о ее температуре, напряжении и внутреннем сопротивлении. На сегодняшний день к одному контроллеру с помощью датчиков можно подключить 200 батарей, но к концу текущего года это количество вырастет до 600, заверяет Алексей Лобов, директор по развитию бизнеса CyberPower.

По его словам, система управления батареями может сыграть важную роль в повышении эффективности крупных ЦОДов. Применение BMS на объектах такого масштаба увеличивает срок службы аккумуляторных батарей до 20%, сокращает время на замену вышедшей из строя батареи на 30% и снижает издержки на эксплуатацию АКБ до 50%.

Однако, какой бы запас надежности не имела инженерная инфраструктура дата-центра, для обеспечения бесперебойного питания оборудования и его охлаждения с минимальными простоями требуется дублировать ИБП дизель-генераторными установками. Выбирая поставщика ДГУ для дата-центров уровня Tier III и Tier IV, нужно обращать внимание на соответствие его оборудования требованиям Uptime Institute для таких объектов, требованиям NFPA 110 и, конечно же, на его оперативную готовность, считает Рустем Давыдов, инженер по применению дизель-генераторных установок компании «МТУ Рус», официального дистрибьютора оборудования MTU.

Для критически важных объектов, коими являются ЦОДы, вендор предлагает ДГУ MTU 2000 мощностью 624–1250 кВт и высокооборотные ДГУ MTU 4000 DS мощностью 1200–3000 кВт. Отличительными особенностями этого оборудования являются высокий предел снижения мощности, высокая приемистость нагрузки, высокая гибкость для сложных индивидуальных решений, а также низкая концентрация загрязняющих веществ в выбросах.

Рецепты экономии на охлаждении

Еще один путь снижения операционных затрат ЦОДов, приобретающий особое значение при увеличении доли высоконагруженных стоек в машзалах, – повышение энергоэффективности систем охлаждения.

Для того чтобы спроектировать «идеальный» ЦОД, по мнению Алексея Харитонова, руководителя технического отдела компании Daichi, мало знать ответы на вопросы, касающиеся выбора принципа построения холодильного центра, производителя оборудования, типа компрессора, его привода и, наконец, алгоритмов работы, поскольку такое знание не гарантирует результат. Необходимо найти основной критерий, принципиально важный для заказчика. В случае с компанией КРОК, которая привлекла Daichi к организации охлаждения своего нового ЦОДа, таким критерием явились минимальные приведенные затраты в течение трех лет эксплуатации.

Для анализа различных вариантов инженерами Daichi была применена специальная методика, основанная на климатических данных. На их базе была составлена таблица, в которой было перечислено все оборудование хладоцентра и для каждой температуры воздуха указано соответствующее значение потребляемой им энергии. В результате изучения таблицы заказчиком была выбрана простая, но энергоэффективная схема системы охлаждения. В рабочем режиме действуют три группы воздушных винтовых инверторных чиллеров Daikin, нагруженных на 60–66%. При выходе из строя одной группы две оставшиеся берут нагрузку на себя и загружаются на 100%, обеспечивая на выходе температуру 15–20°C. При этом в холодных коридорах дата-центра она составляет 22°C. На полный фрикулинг система выходит при +12°C.

Решение оказалось экономически выгодным, поскольку установленная мощность воздушного инверторного чиллера Daikin на 28% меньше, чем у стандартных холодильных машин.

Оптимизацию инвестиций в систему охлаждения ЦОДов обеспечивает правильный выбор между испарительными (мокрыми) градирнями, закрытыми сухими градирнями и гибридными системами, построенными на основе первых или вторых. Опыт известного производителя драйкулеров, немецкой компании Cabero, приобретенный в ходе реализации ряда крупных проектов в Германии и в России, по словам Александры Эрлих, сеньор-консультанта этой компании и генерального директора компании profITcool, говорит о том, что у гибридных аппаратов на основе сухих градирен есть целый ряд преимуществ перед их «мокрыми» собратьями.

Так, «сухие» гибриды хороши тем, что при температуре воздуха до 21°C не требуют использования воды. И даже при максимальных температурах внешнего воздуха потребляют в 2 раза

«Пожтехника» разработала прототип решения иммерсионного охлаждения

меньше воды, что уже обеспечивает экономию этого ресурса. К тому же в режим полного свободного охлаждения такой аппарат переходит при глубоко плюсовых температурах, что дает дополнительно 500–1500 ч работы в режиме фрикулинга в год и также позволяет экономить. Кроме того, драйкулер обходится дешевле решений на основе испарительных градирен на 20–50%.

Еще один вызов для проектировщиков систем охлаждения в дата-центрах – ограниченный размер площадей, выделяемых для этой цели. Иногда эти ограничения связаны с нехваткой площадей, иногда с желанием заказчика отвести больше места под стойки с ИТ-оборудованием. Ответ на вопрос, как организовать энергоэффективную систему охлаждения на небольших площадях, нашли в компании HTS, авторизованном поставщике оборудования прецизионного кондиционирования воздуха и холодоснабжения компании STULZ в России.

В 2017 г. ее специалисты реализовали сразу два проекта, в каждом из которых было найдено решение проблемы ограниченных площадей. Так, в дата-центре «Первой грузовой компании», расположенном в здании ее офиса, они отказались от фреоновых труб в пользу водяного охлаждения, выбрав компактные чиллеры STULZ со встроенной системой фрикулинга. Благодаря наличию насосной группы и теплообменника внутри этих машин их удалось разместить очень компактно. К тому же выбранная конфигурация может около полугода работать с минимальным потреблением электроэнергии.

Заказчиком другого проекта выступила компания SafeDATA, которой было необходимо обеспечить наименьшее потребление энергии при минимизации площади, занимаемой системой охлаждения в ЦОДе «Москва-II». Использование прецизионных кондиционеров STULZ ASR 1360 CW и чиллеров STULZ CSO ESO 12 602 позволило не только решить эту задачу, но и добиться суммарного потребления электроэнергии всех чиллеров на 200 кВт*ч меньше, чем у ближайшего конкурента.

Еще большую экономию площадей, занимаемых в ЦОДах системами охлаждения, а заодно и снижение затрат на их эксплуатацию более чем на 90% обещает переход на технологию иммерсионного, или двухфазного жидкостного охлаждения, разработанную компанией 3M. В состав этой системы входит металлический резервуар, конденсатор с радиатором, управляющие компоненты и сенсоры и охлаждающая жидкость Novec 7100.

По словам Антона Анненкова, исполнительного директора ГК «Пожтехника», эта тихая система без вентиляторов обеспечивает высокие эффективность отвода тепла и теплоемкость, а также возможность использовать энергию тепла повторно, например, для обогрева. Но главное ее преимущество – экономия до 90% затрат на охлаждение и увеличение плотности вычислений на заданной площади.

В настоящее время «Пожтехника», где уже разработан прототип системы иммерсионного охлаждения, ищет партнеров для совместного их продвижения в дата-центры.

■ ■ ■

Словом, поставщики оборудования и решений для инженерной инфраструктуры ЦОДов сегодня активно работают над повышением готовности этих сложных объектов к цифровизации экономики. ИКС

Быть лидером

Для современных ИТ-компаний критически важны непрерывность и эффективность бизнес-процессов. О том, что представляет собой и как развивается ИТ-инфраструктура Электронной торговой площадки Газпромбанка (ЭТП ГПБ), рассказывает Денис Анциферов, управляющий директор ЭТП ГПБ.

– Денис, каковы особенности бизнеса и конкурентной среды для ЭТП ГПБ?

– ЭТП ГПБ – универсальная электронная торговая площадка для реализации закупок в рамках 44-ФЗ, 223-ФЗ и в коммерческом сегменте. Наша торговая площадка – один из лидеров российского рынка электронных закупок, занимает первое место в нефтегазовом секторе с совокупным объемом торгов более 4,5 трлн руб.

Рынок электронных торгов – это высококонкурентная среда. По данным Минэкономразвития России, на конец 2016 г. только в рамках 223-ФЗ работало более 170 площадок. Чтобы оставаться в лидерах отрасли, недостаточно быть лишь местом для проведения торгов. Сейчас рынком востребованы решения, с помощью которых заказчик может автоматизировать весь цикл торгово-закупочной деятельности, от планирования потребности до контроля за исполнением договоров, где проведение самих торгов – лишь один из нескольких этапов. Клиенты ЭТП ждут от площадок дополнительных сервисов, позволяющих повысить эффективность бизнеса: кредитования, факторинга, банковского сопровождения, проверки контрагентов, ведения справочников.

– К каким отраслям принадлежат клиенты ЭТП ГПБ?

– Изначально наша торговая площадка специализировалась на нефтегазовом секторе российской экономики. Однако несколько лет назад ЭТП ГПБ стала межотраслевой, представлена практически во всех отраслях экономики. Среди наших клиентов – «Газпром», «Новатэк», «Уралмаш», ОМЗ, «Мечел», «Мираторг», «Военторг» и другие.

В июле 2017 г. ЭТП ГПБ была интегрирована с государственной информационной системой промышленности (ГИСП) в рамках реализации соглашения о стратегическом партнерстве между Газпромбанком и Минпромторгом РФ. Пользователи ГИСП получили доступ ко всем сервисам ЭТП ГПБ. А в соответствии с Распоряжением Правительства РФ от 12 июля 2018 г. № 1447-р ООО «ЭТП ГПБ» вошло в перечень восьми площадок, на которых с 1 октября 2018 г. могут проводиться государственные закупки в рамках 44-ФЗ.

– Каково место ЦОДа в общей стратегии компании, что представляет собой сегодня ИТ-инфраструктура ЭТП ГПБ?

– ЭТП ГПБ – это ИТ-компания, в основе бизнеса которой лежит предоставление клиентам SaaS-решений для оптимизации торгово-закупочной деятельности. Соответственно дата-центры, в которых размещается программно-аппаратный комплекс основного продукта компании – электронной торговой площадки, имеют ключевое значение для нашей компании.

ЭТП ГПБ имеет SOA-архитектуру (service-oriented architecture), что позволяет нам максимально быстро подстраиваться под требования рынка, своевременно реализуя новый функционал или модифицируя имеющийся независимыми командами разработчиков и применяя наиболее эффективный в каждом конкретном случае стек технологий.

– Финансовые организации долгое время использовали исключительно собственные ЦОДы. Но сейчас они все больше обращаются к услугам коммерческих дата-центров. По каким причинам вы решили обратиться в КЦОД?

– Основная причина выбора коммерческого ЦОДа, а не построения собственного в том, что на российском рынке работают дата-центры, которые в состоянии предоставлять услуги высокого уровня за цену значительно ниже стоимости владения собственным ЦОДом аналогичного уровня.

– Как решались данные задачи до выбора DataSpace в качестве поставщика услуг ЦОДа?

– До переезда в названный дата-центр ЭТП ГПБ успешно пользовалась услугами другого участника данного рынка. Однако в связи с изменением ситуации на рынке электронных торгов и последующим резким увеличением количества клиентов ЭТП ГПБ возникла потребность в многократном увеличении аппаратных мощностей нашей торговой платформы. Параллельно мы давно хотели увеличить надежность нашей системы за счет ее размещения в нескольких ЦОДах. Одной же из основных причин, повлиявших на выбор DataSpace в качестве нашего партнера, послужило то, что данный дата-центр является одним из немногих, доказавших свою эксплуатационную надежность и доступность, в частности, полной сертификацией TIER III объекта в разделах Design, Facility и Operational Sustainability – для нашей компании критически важна уверенность в 100%-ной надежности и доступности нашей электронной торговой площадки с учетом того, что нашими клиентами и партнерами являются такие системообразующие российские компании и государственные структуры, как ПАО «Газпром», Минпромторг России, а также тысячи других российских и зарубежных компаний.

– Каковы были ваши основные требования к площадке КЦОДа? И в чем их специфика?

– Наши основные требования к ЦОДу вполне укладываются в стандарт TIER III Uptime Institute. Но для нас важно, чтобы ЦОД мог подтвердить не только соответствие проектной документации данному стандарту, но и соответствие построенного объекта этим требованиям, а также квалификацию своего персонала.

– Что на сегодня представляет собой ваш ЦОД, размещенный на площадке DataSpace?

– Сегодня он состоит из нескольких стоек с оборудованием от ведущих мировых производителей – HP и Cisco. При этом пространство вокруг дата-стоек физически обособлено и оборудовано, в том числе собственными системами видеонаблюдения и СКУД, что позволяет самостоятельно вести мониторинг окружающей оборудование обстановки в режиме 24x7 и исключить доступ к нему посторонних лиц.

– Сегодня говорят о гибридных схемах, в которых одна часть приложений (данных) остается в ЦОДе компании, а другая выносится в ЦОД провайдера. Вы применяете (планируете использовать) такую схему?

– Мы также применяем эту схему. В нашем случае в собственном ЦОДе мы размещаем резервные банки данных, что позволяет нам дополнительно повысить надежность подсистемы хранения данных. Также там размещена часть ИТ-инфраструктуры компании, которая необходима нашим разработчикам, благодаря чему мы сократили издержки на развитие и поддержку системы, при этом не снизив их скорость и качество.

– Используете ли вы облачную модель? Что выносите в облака?

– Если под облачной моделью подразумевается размещение программных средств в виртуальной среде, то да, в своем решении мы используем средства виртуализации. Это позволяет нам максимально быстро реагировать на изменения внешней среды и своевременно перераспределять имеющиеся у нас в наличии вычислительные ресурсы. Однако мы используем исключительно частные (приватные) облака, т.е. данную виртуальную среду мы разворачиваем на собственных аппаратных средствах – это вызвано тем, что в настоящий момент обеспечить надлежащий уровень информационной безопасности возможно лишь при таком подходе.

– Какие услуги предоставляет ЭТП ГПБ своим клиентам, используя мощности, размещенные в ЦОДе DataSpace?

– Архитектура нашей электронной торговой платформы такова, что добавление нового ЦОДа в ее состав приведет лишь к увеличению производительности и катастрофоустойчивости платформы. Соответственно часть программно-аппаратного комплекса, размещенного в ЦОДе DataSpace, предоставляет своим клиентам весь перечень услуг ЭТП, например, такие как автоматизация всего цикла торгово-закупочной деятельности (формирование и согласование планов закупок, проведение торгов, включая возможность их консолидации в рамках холдинговой структуры, заключение договоров в электронной форме и контроль их исполнения), сопутствующие финансовые сервисы (кредитование, банковские гарантии, факторинг, банковское сопровождение и т.д.), а также аналитика, управление НСИ и справочниками, маркетинг и работа с поставщиками и многие другие.

– Расскажите, пожалуйста, о планах развития ИТ-инфраструктуры ЭТП ГПБ.

– На данном этапе развития наша ИТ-инфраструктура уже отвечает всем предъявляемым к ней требованиям со значительным запасом. Одним из основных подходов к ее построению для нас, так же, как и для внешнего дата-центра, является резервирование всех компонентов системы по схеме 2N, а критически важных – 2N + 1. Дополнительно могу лишь сказать: учитывая, что уже сейчас значимость нашей электронной площадки для российской экономики носит глобальный характер, а также то, что мы являемся одной из немногих электронных торговых платформ, которые в состоянии представлять интересы российских предприятий за рубежом, мы уже сейчас работаем над повышением катастрофоустойчивости нашего решения за счет размещения вычислительных ресурсов и банков данных в разных удаленных регионах России.

Разработка концепции ЦОДа Шаг за шагом

Андрей Павлов, генеральный директор, «ДатаДом»

Дмитрий Басистый, независимый онсультант

На какие вопросы должна дать ответ концепция дата-центра, что нужно в нее включить и в какой последовательности создавать необходимые документы? Авторы делятся опытом, накопленным в ходе выполнения многих проектов.

Функции и состав концепции

Назначение концепции ЦОДа – определение требований к будущему объекту строительства: к его энерговооруженности, площади, количеству стоек, их мощности и уровню надежности инженерных систем. В ходе разработки концепции заказчик получает возможность оценить степень пригодности рассматриваемой площадки (площадок) для строительства дата-центра, а также юридические, физические, технические и иные риски проекта. Техническая оценка состояния площадки выполняется на основе визуального и инструментального обследования территории ЦОДа, включая конструктив здания и прилегающую территорию.

Концепция складывается из целого ряда документов. Помимо определения основных требований к создаваемому дата-центру, в ней, как правило, содержится сравнение вариантов технической реализации тех или иных инженерных систем, дается оценка окупаемости каждого из вариантов и указывается оптимальное решение. Для выбранного технического решения оцениваются бюджеты строительства и эксплуатации объекта. При сравнении различных вариантов строительства (модульный ЦОД, капитальное строительство и т.д.) по требованию заказчика может быть выполнен расчет совокупной стоимости владения (Total Cost of Ownership, TCO) с горизонтом планирования, равным предполагаемому сроку службы объекта. Это поможет заказчику решить, целесообразно ли строить собственный дата-центр или предпочтительнее обратиться к предлагаемым на рынке услугам аутсорсинга. Завершают концепцию рекомендации по выбору того или иного варианта строительства, оценка интегральных рисков проекта и техническое задание на создание дата-центра.

Реестр запрошенных документов

При разработке концепции целесообразно в первую очередь составить реестр запрошенных документов, содержащий перечень предоставленной заказчиком документации, которая необходима для проведения обследования площадки под строительство и оценки рисков проекта.

Поскольку перечень запрашиваемой информации практически не меняется от проекта к проекту, а срок обработки подобных запросов компаниями, обслуживающими здания, может быть достаточно велик, мы рекомендуем начать процесс получения данной информации на самых ранних этапах создания концепции.

Необходимый, но не исчерпывающий перечень требуемой документации

- геоподоснова, справка о геологическом строении и гидрогеологических условиях участка, кадастровый паспорт;
- планы здания, документы, подтверждающие нагрузочную способность перекрытия;
- технические условия на электроснабжение, водоснабжение, канализацию;
- проекты инженерных систем;
- правоустанавливающие документы на здание и прилегающую территорию.

Сформированный реестр в процессе анализа документации и совместной работы с эксплуатирующей здание организацией и представителями собственника должен постоянно актуализироваться.

Методология создания концепции

Следующим документом, на наш взгляд, должна стать «Методология создания концепции». Безусловно, идеально было бы изложить все пожелания заказчика к составу и детализации документа в техническом задании на разработку концепции. Но зачастую в этом техзадании содержатся лишь несколько основных параметров ЦОДа и общее видение проекта, поскольку заказчик может еще не представлять детально, что, а главное, в каком формате должно быть отражено в этом документе.

Во избежание неправильной трактовки содержания результирующих документов, подготовленных в соответствии с договором о разработке концепции, мы рекомендуем создать методологию, в которой будет отражена вся последовательность шагов ее разработки, шаблоны всех выпускаемых документов. Методология может быть приложением к коммерческому предложению на разработку концепции.

Основные характеристики ЦОДа

Этот документ предназначен для уточнения характеристик будущего дата-центра, выбранных еще на этапе техзадания на разработку концепции. Он используется для однозначного формулирования задач по обследованию и экспертизе предполагаемой площадки строительства ЦОДа, выбору технических решений и расчету ТСО. Составление такого документа позволяет значительно снизить риски кардинальной корректировки технических и финансовых расчетов на финальных стадиях разработки концепции.

В число основных мы включаем характеристики ЦОДа, существенно влияющие на параметры площадки под строительство, в том числе на ее площадь и местоположение, нагрузочную способность перекрытий, длины трасс коммуникаций, наличие мощностей ресурсоснабжающих организаций и т.д.

Примерный перечень основных характеристик ЦОДа

- схема резервирования СБЭ (ИБП);
- схема резервирования СГЭ (ДГУ);
- схема резервирования системы кондиционирования;
- мощность ИТ-оборудования;
- общее энергопотребление ЦОДа;
- требуемое время автономии АКБ;
- требуемый запас топлива для ДГУ;
- количество и габариты стойко-мест;
- наличие ИТ-потребителей с постоянным током.

Кроме того, имеет смысл определить вспомогательные характеристики ЦОДа, не влияющие на возможность его возведения на данной площадке, но влияющие на финансовую составляющую строительства.

Перечень вспомогательных характиеристик ЦОДа

- количество и технология портов СКС;
- уровень резервирования систем безопасности;
- необходимость функции сверхраннего обнаружения возгорания;
- требуемые температурно-влажностные режимы работы ИТ-оборудования;
- наличие приточно-вытяжной вентиляции;
- пропускная способность каналов связи;
- количество независимых каналов связи (оптических вводов) и т.д.

Необходимо провести инструментальный обмер территории, прилегающей к зданию ЦОДа, и находящихся на ней сооружений

Перечень основных характекристик ЦОДа формирует, отталкиваясь от бизнес-задач заказчика, рабочая группа, в которую следует включить как экспертов исполнителя, так и представителей заказчика, собственника здания и прилегающей территории объекта, а также представителей эксплуатирующей организации. В документе рекомендуется приводить не только значения выбранных характеристик, но и обоснование их выбора.

Для подтверждения характеристик площадки под строительство и определения ограничений параметров будущего ЦОДа исполнителю следует осмотреть объект с выездом на место. По результатам выезда нужно составить отчет, который будет являться составной частью обоснования выбора основных характеристик ЦОДа и должен быть включен в одноименный документ.

Анализ правоустанавливающих и технических документов

В результате анализа юридических и технических документов, подтверждающих право собственности и условия эксплуатации объекта, должны быть установлены возможность либо невозможность полной/частичной его продажи, вероятность отчуждения и наличие обременений. Также нужно изучить состояние инженерных систем здания, возможность размещения внешних элементов инженерных систем и получения от ресурсоснабжающих организаций ресурсов в количестве, необходимом для строительства и функционирования ЦОДа с заданными параметрами.

В качестве исходных данных для анализа используются документы, которые предоставляют заказчик, собственник здания и эксплуатирующая организация согласно реестру запрошенной документации. Кроме того, часть документации исполнитель может запросить в контрольно-надзорных органах исполнительной власти.

Анализ правоустанавливающих документов проводится в два этапа. На первом этапе оцени-

Стоимость крупного инженерного оборудования составляет более половины всей стоимости проекта

ваются полнота и актуальность собранной и предоставленной документации, после чего делаются выводы о дополнительных рисках проекта, которые могут возникнуть ввиду отсутствия, недостаточности либо неактуальности этой информации.

Факторы, с которыми могут быть сопряжены дополнительные риски проекта

- возникновение права на объекты недвижимости;
- изначальное приобретение прав на объекты недвижимости;
- корпоративные правоотношения;
- технический учет объектов недвижимости;
- выделение помещений в самостоятельные объекты прав;
- наличие ограничений и обременений в использовании объектов недвижимости;
- назначение объектов недвижимости;
- подключение к сетям электроснабжения;
- подключение к сетям водоснабжения и водоотведения;
- подключение к сетям теплоснабжения.

На втором этапе оценивается возможность реализации проекта ЦОДа с заданными параметрами на основе документально подтвержденных характеристик площадки, выявленных в результате изучения предоставленной документации.

Результатом проверки правоустанавливающих и правоподтверждающих документов в отношении объектов недвижимости и инженерных коммуникаций являются выявленные риски проекта и рекомендации по их минимизации.

Отчет о пригодности участка для строительства ЦОДа

Данный документ предназначен для подтверждения возможности строительства на выбранной площадке ЦОДа с заданными характеристиками, в том числе возможности размещения в зданиях и на прилегающих территориях инженерного оборудования. В основе документа лежат результаты двух обследований: инструментального обследования несущей способности здания и строительно-технического обследования прилегающей территории. Кроме того, исходя из выбранных ранее основных характеристик ЦОДа следует определить приблизительные площади его машинных залов и предварительные массогабаритные характеристики инженерного оборудования.

Инструментальное обследование несущей способности здания проводится для определения технического состояния его основных несущих конструкций, возможности размещения в нем инженерных систем ЦОДа, а при необходимости – усиления конструктивных элементов. Подобное обследование можно заказать у специализированных лицензированных компаний, которые берут на себя ответственность за риски, возникающие вследствие некорректного расчета несущей способности перекрытий.

Инструментальное обследование выполняется в соответствии с ГОСТ 31937-2011 Здания и сооружения. Правила обследования и мониторинга технического состояния и СП 13-102-2003 Правила обследования несущих строительных конструкций зданий и сооружений.

Виды работ, которые рекомендуется выполнить в рамках инструментального обследования

- анализ существующих документов, относящихся к зданию;
- обмеры с составлением поэтажных планов и разрезов;
- обследование несущих элементов каркаса здания;
- сбор данных о нагрузках – и существующих, и от вновь возводимого объекта;
- обследование конструкций перекрытий;
- определение прочностных характеристик материалов несущих конструкций здания;
- фотофиксация видимых дефектов строительных конструкций.

Итогом обследования здания с целью определения нагрузочной способности для строительства ЦОДа является заключение, включающее рекомендации по размещению оборудования и усилению несущих конструкций.

Строительно-техническое обследование прилегающей территории необходимо, чтобы определить пригодность участка для размещения оборудования ЦОДа (ДГУ, МЦОД, внешние блоки СКВ, кабельные трассы и т.п.).

Первый этап – это визуальный осмотр территории, прилегающей к зданию ЦОДа, в ходе которого проводится инструментальный обмер самой территории и находящихся на ней сооружений и зданий с архитектурными элементами. На втором этапе посредством инструментальных замеров определяется максимальная нагрузка, которую устанавливаемое на площадке обору-

дование может создать на покрытие прилегающей территории без вреда для него и расположенных ниже коммуникаций.

Этапы обследования прилегающей территории для определения максимальной нагрузки

- визуально-инструментальный контроль дефектов и повреждений;
- выявление площадей, свободных от подземных коммуникаций и пригодных для установки инженерного оборудования;
- контрольные вскрытия слоев с определением типов материалов и геометрических характеристик;
- контрольные вскрытия бетонной плиты основания площадки для выявления армирования;
- определения прочностных характеристик бетонной плиты основания;
- экспертный сбор планируемых нагрузок на плиту основания площадки;
- проведение поверочных расчетов несущей способности плиты по грунту под планируемые нагрузки;
- камеральная обработка данных;
- выдача отчета с выводами и рекомендациями.

После анализа документов, описывающих характеристики участка и здания, визуального осмотра и инструментального обмера можно будет определить возможные места установки ДГУ, внешних блоков системы холодоснабжения, прокладки кабельных трасс и т.д. Также на данном этапе можно разработать эскизный план с расположением оборудования.

Реестр рисков

После визуального и инструментального обследования зданий и площадок под строительство, анализа юридической и технической документации рекомендуется свести всю полученную информацию в единый документ – «Реестр рисков». При его составлении целесообразно использовать экспертные оценки наличия тех или иных рисков строительства и функционирования объекта, которые на основании опыта проектирования, строительства и эксплуатации дата-центров может сделать исполнитель, а также лучшие мировые практики. К анализу проектных рисков также могут быть приглашены сторонние эксперты отрасли ЦОДов.

Первым шагом при анализе внешних рисков должна стать экспертная оценка вероятности их реализации и степени влияния на проект строительства ЦОДа на выбранных площадках. Следующий шаг – ранжирование и оценка значимости каждого из выявленных рисков и разработка экспертных заключений о возможных мерах их устранения.

Результатом данного этапа работ должен являться реестр рисков, связанных с расположением объекта и его инженерным обеспечением, который разработан для различных вариантов строительства ЦОДа с оценкой значимости каждого риска, а также выводы и рекомендации по минимизации их влияния на проект. Если критических рисков в перечне окажется много, рабочая группа может принять решение о нецелесообразности строительства ЦОДа на выбранной площадке.

Приблизительный перечень категорий рисков, которые нужно учитывать при принятии решения о строительстве ЦОДа

- планировка и конструктивные решения здания;
- внешнее электроснабжение;
- доступность телекоммуникационной инфраструктуры;
- окружение площадки;
- отсутствие актуализированной информации;
- физическая безопасность;
- транспортная доступность, пути подъезда;
- юридические риски;
- финансовые риски.

Разработка и сравнение вариантов технических решений ЦОДа

Наконец мы приступаем к созданию основных технических документов, которые будут содержать подробное описание различных вариантов инженерных систем, сравнение их технико-экономических показателей, обоснование выбора той или иной технологии энергоснабжения, холодоснабжения и т.д.

Для оптимизации объема предстоящей работы рекомендуем изначально оценить степень критичности инженерных систем ЦОДа и их влияние на стоимость проекта и его реализуемость на выбранной площадке. Очевидной задачей концепции является оценка возможности создания дата-центра и бюджета строительства, поэтому те инженерные системы, которые занимают в общей стоимости проекта менее одного процента и при этом не влияют на площадь ЦОДа (к примеру, СКУД, охранная сигнализация), могут быть рассмотрены гораздо менее детально, нежели, например, система кондиционирования. Для разных ЦОДов состав некритичных систем может различаться, скажем, доля СКС в бюджете строительства банковского ЦОДа может быть существенной, а для коммерческого ЦОДа – крайне незначительной.

Рекомендуем описать основные принципы взаимодействия инженерных подсистем, что будет хорошим подспорьем для заказчика с точки зрения однозначного понимания правил функционирования дата-центра. Особое внимание следует уделить описанию строительной подготовки помещения ЦОДа, либо, что еще более важно, капитального строительства, так как это является базой разрабатываемой концепции

и может существенно повлиять на стоимостные и временные параметры проекта.

Далее мы переходим к непосредственному сравнению и выбору критических инженерных систем и описываем некритичные системы. Для каждой критичной системы приводятся ретроспектива возможных технических решений, предлагаемых на рынке, принципы функционирования каждой из них, расчеты основных технических параметров, оценки стоимости. Для указанных вариантов реализации сравнивается стоимость владения, даются обоснования и рекомендации по выбору той или иной технологии. В приложениях к разделу должны содержаться объемно-планировочные решения для выбранных технических реализаций ЦОДа. Также мы рекомендуем рассчитать общее энергопотребление и параметр PUE проектируемого дата-центра.

В заключении данного раздела необходимо описать состав комплекса инженерных систем ЦОДа с информацией по отдельным системам, их назначению и выбранным техническим решениям.

Расчет совокупной стоимости владения

Как отмечалось выше, в рамках концепции может быть рассчитана TCO. Стоимость основного инженерного оборудования ЦОДа (ИБП, ДГУ, кондиционеры, АКБ, СГП, СКС) можно определить исходя из альтернативных коммерческих предложений его поставщиков на российском рынке. Для подтверждения стоимости этого оборудования мы, как правило, предоставляем несколько коммерческих предложений из разных ценовых сегментов. Остальные инженерные системы, в сумме составляющие менее 30% общей стоимости ЦОДа, мы оцениваем экспертно, на основании имеющегося опыта строительства.

Совокупная стоимость владения складывается из двух составляющих:

$$TCO = CAPEX + OPEX.$$

CAPEX (capital expenditure, капитальные затраты) – это затраты на приобретение необоротных активов, а также на их модификацию (достройку, дооборудование, реконструкцию) и модернизацию. Сюда относятся и затраты на проектирование, строительство, поставку оборудования и т.д.

OPEX (operational expenditure, операционные затраты) представляют собой затраты компании, которые возникают в процессе ее текущей деятельности, – затраты на заработную плату сотрудников, текущий ремонт, энергоресурсы, налоги и пр.

На этапе концепции мы оцениваем порядок величины затрат (отличие от реальной стоимости примерно ±20%). Для его определения применяется смешанный метод, совмещающий оценку «по аналогу» с параметрическим методом. Благодаря тому, что стоимость крупного инженерного оборудования, которая составляет более половины всей стоимости проекта, известна, точность оценок повышается.

Статьи расходов, включаемые нами в показатель CAPEX

- разработка технического проекта;
- получение технических условий на подключение внешних коммуникаций;
- разработка рабочей документации;
- проведение государственной экспертизы;
- проведение конкурса по выбору генерального подрядчика;
- реализация технических условий на подключение внешних коммуникаций;
- ремонт капитальных сооружений и благоустройство площадки;
- переезд офисов и иные организационные меры;
- строительство инженерной инфраструктуры.

Статьи расходов, относящиеся OPEX

- фонд оплаты труда персонала ЦОДа;
- ЗИП;
- плановые ремонты;
- услуги технической поддержки вендоров и специализированных организаций;
- обучение персонала;
- оплата электроэнергии и иных ресурсов;
- ликвидация аварий и аварийные ремонты;
- общехозяйственные расходы.

На основе этой информации рассчитывается ежегодный показатель TCO на срок предполагаемой службы ЦОДа.

Заключение и техническое задание на создание ЦОДа

В финальном документе концепции – «Заключении» – мы представляем всю информацию, полученную на предыдущих этапах работы, в виде краткой выжимки с отсылками к соответствующим документам, что позволяет заказчику проследить весь ход исследования объекта строительства – от выбора параметров дата-центра до эскизного проекта, имея возможность более детально изучить интересующие его этапы, переходя по ссылкам на базовые документы. В «Заключении» приводится итоговое техническое решение строительства ЦОДа с техническим и экономическим обоснованием выбора конкретного варианта строительства, с планировочными решениями и обоснованием бюджета и сроков реализации проекта.

На основе принятой и утвержденной концепции может быть разработано техническое задание на создание/проектирование ЦОДа, включающее в себя все выбранные технические решения и основные и вспомогательные характеристики будущего дата-центра. ИКС

Rittal – The System.

Faster – better – everywhere.

Самая компактная установка IT-охлаждения Rittal в своём классе

- Расположение непосредственно внутри шкафа
- Оптимальное движение воздуха «спереди-назад»
- Два класса мощности в одном типоразмере
- Возможность резервирования
- Инверторные и EC технологии
- Выносной наружный блок

Обеспечение необходимого для IT потока воздуха «спереди-назад». Инверторное управление компрессором и EC вентиляторы для достижения максимальной энергоэффективности и точности поддержания параметров.

«Сплит» исполнение без нагрева внутреннего воздуха. Гибкое расположение наружного блока. Максимальное расстояние до 50 метров.

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

FRIEDHELM LOH GROUP

www.rittal.ru

RITTAL

Итальянцы в России

Климатическое оборудование итальянской компании HiRef хорошо известно на российском рынке. В ближайшее время в нашей стране официально откроется офис компании и стартует производство ее продукции. Планами делится Василий Новиков, директор по развитию HiRef RUS.

Василий Новиков

– Василий, давайте сразу о главном: где и что будет производиться?

– Спрос на современное холодильное и климатическое оборудование, в том числе для ЦОДов, в России стабильно растет. Существующий успешный опыт реализации продукции HiRef на территории РФ и постоянно растущий спрос на нее стали отправными точками для принятия руководством HiRef Италия решения о локализации производства именно на территории РФ. Самое пристальное внимание уделялось выбору производственной площадки, на базе которой планируется организовать выпуск продукции, ведь во главу угла компания HiRef ставит качество изготавливаемого оборудования.

Такой площадкой, отвечающей всем необходимым критериям, стал завод «Рефкул», расположенный в непосредственной близости от Москвы, на территории ОЭЗ в Калужской области. Этот завод оснащен передовым технологическим оборудованием, существующий станочный парк позволяет реализовать полный производственный цикл в рамках одной площадки. Высококвалифицированный персонал завода «Рефкул» имеет большой опыт в сборке аналогичного оборудования и в дальнейшем будет регулярно проходить обучение за заводах группы HiRef в Италии. Производство на всех его этапах будет контролироваться итальянскими специалистами HiRef, что обеспечит высокое качество выпускаемой продукции, соответствующее мировым стандартам HiRef.

Первое оборудование российской сборки сойдет с конвейера уже в начале 2019 г. Это будут самые востребованные, превосходно себя зарекомендовавшие на российском рынке модели прецизионных кондиционеров шкафного типа серии JREF и TREF. В дальнейшем линейка выпускаемой продукции будет постоянно расширяться.

– Каковы преимущества производства в России?

– Их масса, и мы надеемся, что наши клиенты по достоинству их оценят. В существующих российских реалиях концепция импортозамещения с каждым годом становится все более актуальной для наших клиентов не только из государственного, но и из коммерческого сектора. Общая тенденция на рынке такова, что все больше заказчиков отдают предпочтение продукции, произведенной на территории России. Наша компания готова предложить не просто оборудование отечественного производства, но прежде всего его неизменно высокое качество, самые передовые технологии, услуги сервисного, гарантийного и постгарантийного обслуживания с использованием запасных частей, находящихся в свободном доступе на территории РФ; техническую поддержку непосредственно от производителя, удобную логистику и оптимальные сроки поставки. Клиенты могут принять участие в предварительных испытаниях продукции перед ее отправкой, что зачастую является обязательным условием поставки продукции на предприятия оборонного и нефтехимического комплекса.

Немаловажный фактор – цена продукции. Собственное производство на территории России позволит сделать цены на оборудование HiRef максимально привлекательными, а также снизит влияние валютных колебаний на рынке на стоимость продукции.

Очевидны и логистические преимущества, которые предоставляет локализованное производство. Когда европейский завод работает на весь мир, нередки неизбежные трудности с оперативным выполнением заказов, обусловленные высокой загрузкой производства и длинной логистической цепью. В среднем срок производства кондиционера у любой компании составляет четыре-шесть недель. В пик сезона этот показатель может увеличиваться до 12–14 недель. Наличие производства в России позволит этого избежать, а кроме того, обеспечит возможность предложить более разнообразные условия доставки продукции.

Безусловно, наши клиенты по достоинству оценят все преимущества наличия у производителя на территории РФ собственной службы технической поддержки, а также сервисной службы.

Наши заказчики будут иметь возможность получать уникальные услуги: мы планируем внедрить систему хранения технической сопроводительной документации для каждой единицы произведенной продукции. В любой момент заказчик сможет обратиться напрямую к производителю за копией технической документации, которая зачастую не попадает к конечному пользователю в полном объеме. Любой покупатель оборудования HiRef сможет получить техническую консультацию по вопросам эксплуатации нашего оборудования, воспользоваться услугами сервисной службы, в том числе получить услуги шеф-монтажа и пусконаладки.

Обычно при возникновении каких-либо вопросов по работе оборудования цепочка взаимодействия выглядит следующим образом: конечный клиент → продавец → дилер → дистрибьютор → завод-производитель.

Небольшим региональным заказчикам приходилось сталкиваться с проблемами, связанными с поддержкой оборудования, когда не были произведены его квалифицированный монтаж, сертифицированный запуск и обслуживание.

В нашем случае любой из участников цепочки может сразу напрямую обратиться к производителю, будучи уверенным в том, что все его проблемы, касающиеся эксплуатации оборудования, будут решены в максимально короткий срок.

Мы также планируем на регулярной основе проводить обучающие и технические семинары, на которых будем делиться передовыми наработками HiRef с нашими действующими и потенциальными клиентами. В открытом диалоге всегда легче понять потребности наших клиентов и удовлетворить их.

– Так российский офис HiRef уже работает?

– Компания «Хайреф Рус» официально зарегистрирована в августе 2018 г. Сейчас мы решаем организационные вопросы в преддверии запуска производства оборудования HiRef на заводе «Рефкул». Также мы занимаемся продвижением бренда и оборудования HiRef на российском рынке.

– Вы уверены в сохранении европейского качества при производстве в России?

– Прежде всего хочу отметить, что компания HiRef стремится принести итальянскую культуру инноваций при производстве оборудования на территорию России. Компания HiRef никогда не будет передавать свою продукцию для выпуска на производственную площадку, не будучи уверенной в возможностях производителя обеспечить высокий уровень выпускаемой продукции и ее соответствие всем стандартам компании HiRef Италия. И, безусловно, мы уверены в своем партнере – заводе «Рефкул». Технология производства оборудования HiRef на заводе «Рефкул» идентична технологии производства на заводе HiRef в городе Падуя. Специалисты, которые будут работать на заводе «Рефкул», пройдут специальное обучение в Италии. Все производимое на территории РФ оборудование будет протестировано на собственных испытательных стендах до момента его передачи клиенту.

При производстве оборудования в России будут использоваться только качественные комплектующие, зарекомендовавшие себя на рынке. К примеру, планируется использовать компрессоры Danfoss и Bitzer; автоматику и контроллеры Carel, ABB и Siemens; теплообменное оборудование ebmpapst и Ziehl-abegg. Я уверен, эти компании не нуждаются в представлении, а производимая ими продукция является эталоном качества.

– Почему для производства на первом этапе были выбраны именно названные выше системы?

– Вполне логично, что мы планируем начать производство в России с относительно простого и доступного оборудования. По опыту наших заказчиков, наиболее востребованы фреоновые модели шкафных кондиционеров небольшой мощности JREF DX (7–25 кВт) и TREF DX (27–142 кВт). Дальнейшее расширение производства мы планируем вводить поэтапно, в соответствии со спросом на те или иные системы.

– Речь идет о выпуске «простых» фреоновых систем. А какие планы на выпуск более сложных и энергоэффективных решений для ЦОДов? В России нет спроса на «зеленые» решения?

– Безусловно, в РФ будут выпускаться и водяные системы, и чиллеры, и все остальное. Сборка водяного блока прецизионного кондиционера даже проще, чем фреонового. Но такие решения имеет смысл производить только под конкретный проект. В то же время фреоновые решения в диапазоне мощностей до 50 кВт за время существования склада показали очень неплохую оборачиваемость за счет наличия, невысокой цены и простоты монтажа. Поэтому было решено начать с них.

В применении «зеленых» решений и технологий Россия уступает Европе, где вся климатика «затачивается» под «зеленые» технологии. Но они существенно дороже, а для большинства российских заказчиков CAPEX пока на первом месте.

Вместе с тем, будучи европейским производителем, HiRef уделяет приоритетное внимание энергоэффективным технологиям. В качестве примера приведу чиллеры TTX и XTW, в которых используются безмасляные центробежные компрессоры и затопленные теплообменники. Сочетание этих элементов позволяет максимально повысить эффективность теплообмена – благодаря отсутствию масла в контуре и уменьшенному перепаду температур между водой и хладагентом из-за отсутствия перегрева в испарителе.

Для ЦОДов в контейнерном исполнении HiRef разработала крышные кондиционеры с непосредственным охлаждением. Использование EC-вентиляторов в испарительной секции в связке с системой прямого свободного охлаждения и BLDC-компрессором позволяет максимально увеличить энергоэффективность агрегата, особенно при частичной нагрузке.

Упомяну также наши воздушные системы охлаждения с перекрестным рекуператором HDB-DataBatic. При температуре окружающего воздуха до 21°С они обеспечивают охлаждение ИТ-оборудования исключительно в режиме фрикулинга. При более высоких температурах включается модуль адиабатического охлаждения. При необходимости в HDB-DataBatic задействуется и модуль механического охлаждения.

Замечу, что у HiRef широчайшая гамма климатического оборудования. Помимо прецизионных кондиционеров, она включает чиллеры и геотермальные тепловые насосы. Если заказчику по каким-либо причинам важно получить именно системы из России, то мы готовы оперативно рассмотреть вопрос размещения производства практически любого оборудования из портфеля HiRef уже с начала 2019 г.

– Какова ситуация на российском рынке климатического оборудования для ЦОДов в целом, и как она изменится в связи с обсуждаемыми инициативами HiRef?

– Как я уже говорил, рынок растет. Этому во многом способствует цифровизация всех аспектов нашей жизни. Амбициозные цели по развитию российской индустрии ЦОДов ставят принятая государством программа «Цифровая экономика РФ» и «закон Яровой», реализация которых станет катализатором ускоренного роста.

В настоящее время на российском рынке климатических систем для ЦОДов доминируют четыре основных бренда, включая HiRef. Это все именитые европейские производители. Есть и примеры разработки подобного оборудования отечественными компаниями. Но российской альтернативы оборудованию европейского качества мы пока не наблюдаем.

С нового года такое оборудование появится. С учетом уже названных выше преимуществ локальной сборки с сохранением европейского качества мы рассчитываем существенно увеличить долю HiRef на российском рынке и в странах Таможенного союза.

Кругом вода,
или Соблюдение коридора влажности в системах круглогодичного фрикулинга

Александра Эрлих,
сеньор-консультант,
CABERO

Какие нюансы нужно принять во внимание при проектировании системы круглогодичного фрикулинга, чтобы оптимизировать энергопотребление и в то же время создать комфортные условия для работы как ИТ-оборудования, так и персонала?

До поры до времени ЦОДы работали в определенном режиме влажности и температуры и чувствовали себя в нем довольно комфортно. Но Американская ассоциация инженеров по отоплению, охлаждению и кондиционированию воздуха (American Society of Heating, Refrigerating and Air-Conditioning Engineers, ASHRAE) провела ряд исследований, позволивших – ура! – снова повысить температуру в ЦОДах.

А тут еще выход на рынок систем охлаждения Kyoto Cooling, которые так замечательно работают в ряде стран северо-запада Европы. Возникло понятное желание применить подобные системы в России. Появились первые аналоги, а вместе с ними и первые проблемы.

С Kyoto Cooling у меня особые отношения. Я как раз заканчивала Одесскую академию холода, когда общество всколыхнул феномен так называемой озоновой дыры. Тогда, в 1995–1997 гг., мир науки и техники тоже жил относительно уравновешенно, без революционных скачков и резкого роста выпуска холодильного и климатического оборудования. Киотский протокол буквально взорвал привычный порядок и на долгие десятилетия дал повод менять отличную технику на более современные, но менее совершенные аналоги. Было проведено огромное количество исследований, защищены десятки тысяч диссертаций и обеспечены сотни тысяч рабочих мест в производстве холодильного и климатического оборудования.

Когда в 2010 г. началось массированное продвижение новой технологии фрикулинга – Kyoto Cooling, – понятно, что первой реакцией у меня, как, возможно, и у вас, был скепсис.

Тем не менее технология живет, развивается и довольно успешно применяется, например, в Риге, в ЦОДе Lattelecom. Особенности местного климата в виде постоянных ветров усиливают энергосберегающий эффект такого вида охлаждения – большую часть времени года вентиляторы вращаются естественным путем, не потребляя электричества.

За последние годы технологию развили и адаптировали под разные климатические зоны и требования. Например, в Мюнхене, где температуру воздуха летом можно сравнить с температурами на российском Черноморском побережье, фрикулинг работает 90% времени в году без применения дополнительного компрессорного охлаждения. Снижаются затраты на эксплуатацию ЦОДа, улучшаются показатели PUE, можно красиво рекламировать себя и радовать клиентов ощутимо низкими ценами предоставляемых услуг.

Но у таких систем есть одна проблема – влажность. Этот параметр для дата-центра не менее важен, чем температура.

Какая влажность должна быть в ЦОДе

Если влажность слишком низкая, возникает опасность накопления статического электричества. Считается, что в момент разряда оно может повредить электронные компоненты серверов. Последние исследования ASHRAE доказали, что нижний порог влажности можно снизить до 15% при условии соблюдения элементарных правил безопасности, таких как специальное покрытие пола, обувь, антистатические браслеты и соблюдение температурных норм, рекомендованных той же ASHRAE.

Правда, встает вопрос, насколько вы хотите заниматься соблюдением всех предписанных мер предосторожности, рискуя сбоем самого ненадежного звена любой технологии – пресловутого человеческого фактора.

Однако тема этой статьи не пониженная влажность, которую в худшем случае можно повысить с помощью обычных увлажнителей. Сегодня мы поговорим о верхнем пороге влажности, а именно о том, как соблюсти его в условиях круглогодичного фрикулинга.

Повышенная влажность чревата выпадением конденсата, формированием дождевых облаков, как однажды произошло в ЦОДе Facebook*, в экстремальных случаях – коротким замыканием. В Германии при применении свободного охлаждения вместе с влажностью в ЦОДы пришла еще одна проблема, типичная для развитого капитализма, – плесень. Запад загнивает, причем в буквальном смысле ☺.

Не забудьте также ограничения, в том числе по влажности, которые накладывают на рабочие режимы серверов их производители. И, конечно, коррозию металлов никто не отменял.

Но даже если вы используете материалы, устойчивые к плесени и коррозии, работаете на серверном оборудовании, спроектированном специально для вас, не боитесь короткого замыкания, то вам все равно важно энергопотребление ЦОДа. Иначе вы не затевали бы круглогодичный фрикулинг, верно? А вот как раз этот показатель при повышенной влажности сильно возрастает, поскольку аппаратное обеспечение, пытаясь регулировать конденсацию, серьезно увеличивает потребление электроэнергии по сравнению с «нормальным» режимом.

Речь идет не о кратковременных скачках влажности, а о постоянном ее повышении в машинном зале. В 99% случаев причиной является не сам круглогодичный фрикулинг как способ охлаждения, а ошибки, допущенные при проектировании такой системы. Все-таки системы круглогодичного фрикулинга – явление в мире ЦОДов относительно новое, количество подобных систем и, следовательно, накопленный опыт невелики.

А как в Германии?

Возможно, в такой ситуации проще отказаться от идеи и применить традиционную схему. А можно воспользоваться опытом зарубежных коллег, например, из Германии. Почему именно из Германии? В данном случае не столько потому, что я здесь живу и имею возможность общаться с практиками лично, сколько потому, что именно в этой, самой консервативной и задавленной нормами и законами по строительству и проектированию ЦОДов (их тут более 20) стране Западной Европы, стране с совсем не северным климатом, системы круглогодичного фрикулинга получили широкое распространение.

Посмотрим, на какие аспекты при проектировании обращают внимание немецкие коллеги. Для примера возьмем климатическую зону Мюнхена и принятый в Германии диапазон влажности 25–60%. Имеет значение каждая мелочь, включая количество процессоров с малой / большой тепловой нагрузкой, верхний температурный порог их работы, воздушные потоки в серверном шкафу и в машинном зале, достижимую степень изоляции помещения и отдельных его участков, экстремально возможные значения температуры и влажности наружного воздуха, невозможность полностью избежать подмешивания наружного воздуха, теплопритоки, в том числе от самого климатического оборудования, и многое, многое другое.

Разработка концепции

Проще всего было бы спроектировать систему со стабильным воздушным потоком, подобрать и настроить технику один раз и больше не менять настройки. Но снова вмешивается человеческий фактор: люди, находящиеся в серверной комнате, затрудняют оптимизацию системы, направленную на значительное снижение потребности в энергии для кондиционирования воздуха посредством фрикулинга. Людям нужно дышать, они выделяют определенное количество тепла и углекислого газа, температурно-влажностный режим в машинном зале должен быть для них комфортным, они могут задержаться в дверях дольше, чем считается нужным, забыть что-то и вернуться. Да и количество посещений машзала точно предсказать невозможно.

* Согласно данным The Register, инцидент имел место в ЦОДе в Прайнвилле (шт. Орегон, США) летом 2011 г.

Кроме того, зачастую в разных частях зала необходимо поддерживать разные температурно-влажностные режимы, определяемые непосредственно ИТ-оборудованием (например, в коммерческом ЦОДе). С этой целью в Германии создают систему так называемого двойного фрикулинга.

Суть заключается в следующем: для каждого ЦОДа создается индивидуальная система plug-and-play, способная работать как в режимах прямого и непрямого фрикулинга, так и в режиме компрессорного охлаждения. Она включает в себя системы увлажнения и осушения и способна одинаково хорошо функционировать в режиме и частичной, и полной нагрузки. При этом система обеспечивает значение PUE = 1,2 и ниже.

Вводные для проектирования установки

Самое важное – правильно определить разность между температурой на выходе из горячего коридора и температурой на входе в холодный коридор (Δt). В случае, когда нужно перейти на компрессорное охлаждение, Δt выбирается равной 12 К. При фрикулинге Δt можно и нужно взять больше (но не более 20 К), чтобы сократить объем требуемого воздуха и, как следствие, энергопотребление системы. И конечно, совершенно необходимо собственно разделение коридоров.

Система вентиляции должна быть спланирована таким образом, чтобы, используя различные пути воздушного потока, направлять воздух только туда, где он в настоящее время нужен, и уменьшать за счет этого внутреннее сопротивление потока. Благодаря как минимум двум параллельным воздушным потокам можно, например, создать различные воздушные смеси с различными температурно-влажностными режимами. Обязательно нужно предусмотреть возможность работы установок в режиме частичной загрузки. По возможности задействовать бо́льшее количество малых установок.

Важно: системы прямого фрикулинга могут обеспечивать те же показатели при более высоких температурах наружного воздуха, чем системы непрямого фрикулинга.

Требования к геометрии зала

Как уже говорилось ранее, разделение коридоров является абсолютной необходимостью для создания подобного рода систем. В настоящее время уже следует идти дальше и разграничивать не только коридоры, но и зоны с разными температурно-влажностными режимами.

Второе необходимое условие – переход от фальшпола к фальшпотолку. Вспомним школьную физику: теплый воздух поднимается вверх сам по себе, не требуя дополнительных энергетических затрат. Поэтому выдуваем холодный воздух непосредственно в холодный коридор, позволяем ему подниматься вверх и регулируем воздушные потоки системой клапанов и воздуховодов. Подобное решение круглогодичного фрикулинга уже несколько лет успешно применяется, в частности, в центрах обработки данных одной из крупнейших российских интернет-компаний.

В Германии поток воздуха регулируют не только с помощью механических систем, но и изменяя Δt в соответствии с изменением холодильной нагрузки.

От стандартной установки – к «индпошиву»

Если внимательно изучить требования к системе, становится понятным, что ни одна стандартная установка таким требованиям полностью соответствовать не может. Поэтому не жалеем денег на CAPEX, понимая, что получим замечательно низкий OPEX, и разрабатываем индивидуальную установку. Тем более что даже индивидуальная установка для системы круглогодичного фрикулинга обойдется дешевле, чем стандартный набор, включающий в себя чиллеры, прецизионные кондиционеры, драйкулеры и вспомогательное оборудование.

Возьмем в качестве примера относительно простую установку, например, для ЦОДа общественной организации с гомогенным ИТ-оборудованием.

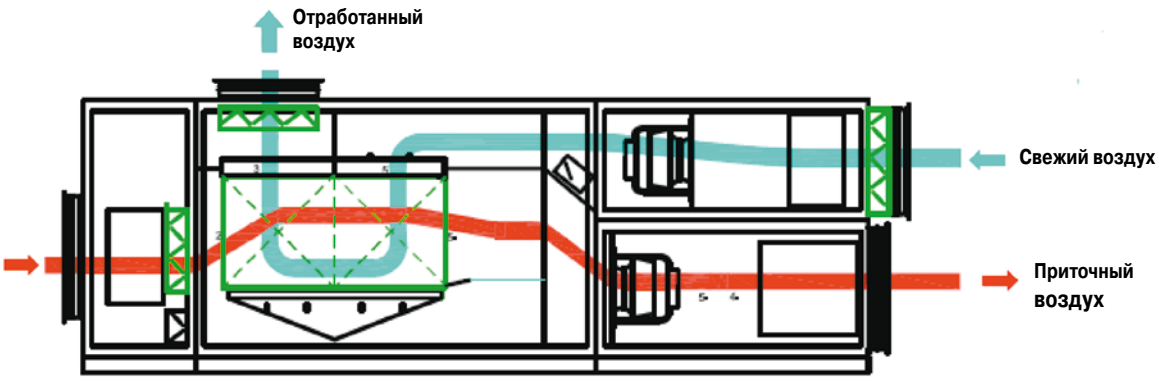


Рис. 1. Непрямой фрикулинг

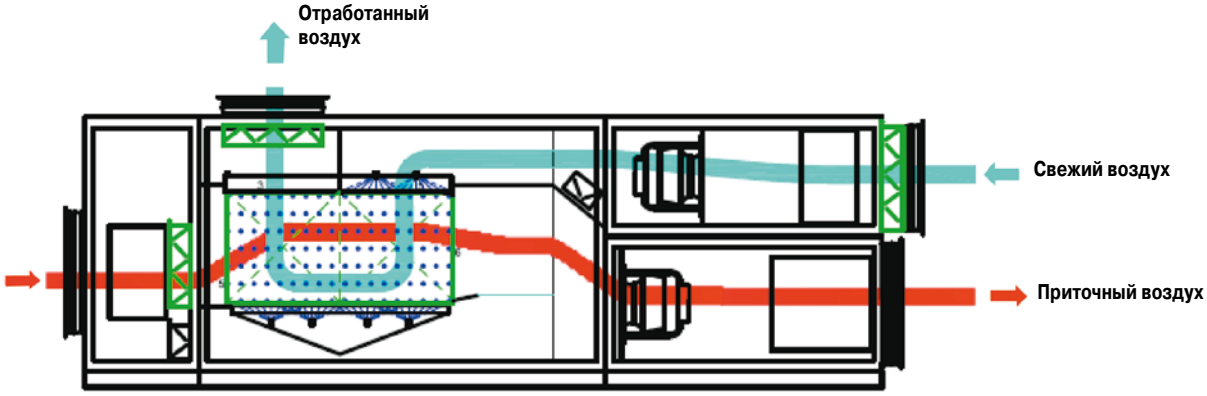


Рис. 2. Фрикулинг с увлажнением

Для круглогодичной работы установки определяют восемь различных штатных режимов и маркируют в h,x-диаграмме. Для каждого из штатных режимов рассчитываются оптимальные параметры, которые учитываются при разработке установки и вносятся в программное обеспечение автоматики. Вентиляторы, теплообменники и клапаны для каждого из этих режимов регулируются отдельно, с акцентом на минимизацию энергопотребления, причем для снижения энергопотребления вентиляторов проводят смешение различных параллельных воздушных потоков.

В качестве штатных режимов могут быть выбраны, например, следующие:

Непрямой фрикулинг. Этот режим (рис. 1) хорош при низких температурах наружного воздуха и соответственно низкой абсолютной влажности. Весь объем воздуха проходит через рекуператор, отбирая через стенку тепло у внутреннего воздуха машзала и отводя его на улицу. Небольшое количество наружного воздуха подмешивается к внутреннему. В таком режиме практически не нужно увлажнение либо осушение.

Прямой фрикулинг. Этот режим применяется при средних температурах наружного воздуха и абсолютной влажности не более 10 г/кг. В климатических условиях Мюнхена в режиме прямого фрикулинга работают примерно полгода. При разработке климатической установки под этот режим нужно учитывать потери давления потока и стараться сделать их минимальными. Наружный воздух в этом режиме не проходит через рекуператор, а параллельным путем через систему фильтров К7 заходит в машинный зал.

Прямой фрикулинг с увлажнением. В случае, когда абсолютная влажность падает ниже 4 г/кг, наружный воздух дополнительно увлажняется (рис. 2).

Адиабатическое увлажнение. Как только температура наружного воздуха становится выше допустимой температуры входящего воздуха, включается режим адиабатического увлажнения, позволяющий дополнительно снизить температуру на 5К.

Испарительное увлажнение. В последнее время вместо адиабатического увлажнения все шире используют непосредственное испарение на рекуператоре специальной конструкции, позволяющее сбить температуру наружного воздуха на 10–12 К. Системы с сотовыми увлажнителями из-за возникновения больших потерь в воздушном потоке (и, как следствие, высокого энергопотребления), а также из-за необходимости частой замены получили менее широкое распространение.

Компрессорное (до)охлаждение. Когда температура наружного воздуха даже после испарения поднимается выше допустимой температуры входящего воздуха, возникает необходимость в компрессорном (до)охлаждении. При этом воздух охлаждается до температуры ниже необходимой, проходя через встроенный конденсатор, охлаждает теплообменный аппарат и параллельно «подсушивается».

Полное компрессорное охлаждение. Если температура воздуха на улице поднялась выше температуры в горячем коридоре, подача наружного воздуха перекрывается, и внутренний воздух охлаждается исключительно встроенной холодильной машиной.

Осушение. В случае, когда содержание водяных паров в воздухе превышает 12 г/кг, наружный воздух принудительно осушается. Для осушения можно задействовать разные системы, начиная с применяемых в бассейнах и заканчивая приборами, разработанными для специальных лабораторий. Но самый простой и дешевый способ – использовать в качестве осушителя встроенную в установку холодильную машину.

Циркуляционное воздушное охлаждение. Предусматривается в качестве аварийного на тот случай, если по каким-либо причинам (например, пожар на улице) наружный воздух независимо от его температуры использовать невозможно. ИКС

Управление жизненным циклом для изменяющихся инфраструктур

Андрей Ивашов, руководитель по развитию направления DCIM подразделения IT Division, Schneider Electric
Андрей Крюков, системный инженер подразделения IT Division, Schneider Electric

Рост числа контролируемых объектов и устройств, повышение требований к безопасности и эффективности, а также дефицит кадров заставляют использовать новый подход к эксплуатации ЦОДов и управлению ими. В его основе – автоматизация, прогнозный мониторинг и предиктивное обслуживание.

Цифровизация неуклонно охватывает все сферы нашей жизни и деятельности. Национальная программа «Цифровая экономика РФ» подразумевает выполнение шести федеральных проектов и привлечение более чем 2,1 трлн руб. Сравним этот бюджет (около $30 млрд) с другими суммами, фигурирующими в ИТ-индустрии. Стоимость самого крупного ЦОДа Microsoft – около $1 млрд, а объем всего мирового рынка оборудования для ЦОДов – $150 млрд. Еще $30 млрд – это доход всех российских коммерческих ЦОДов за 100 лет, точнее – в сто раз больше текущего годового дохода. Сложно представить, сколько средств будет затрачено на инженерную инфраструктуру, но есть уверенность в том, что на рынке будет потребность в современных решениях.

Рано или поздно информационная инфраструктура России вырастет в разы: расширится географическое покрытие, увеличатся объемы хранимых и обрабатываемых данных, количество потребляемой энергии. Прямым следствием будут растущие потребности в кадрах, решениях по безопасности, технологиях энергосбережения и управления жизненным циклом, решениях, снижающих риски и повышающих эффективность. Вполне возможно прогнозировать тенденции технологического развития страны – достаточно следить за мировыми новостями технологий и российскими ИТ-лидерами.

Современные ЦОДы уходят от схем «каждому отделу свое оборудование» и «каждому приложению свой сервер». Кластеризация (объединение вычислительных мощностей) и виртуализация позволили повысить утилизацию стойко-мест и ЦОДов в целом. Но как будет реализовываться новая ИТ-инфраструктура в ближайшие годы? Мы ожидаем увидеть два основных подхода:

- Гиперконвергентный – объединение всего ИТ-оборудования (СХД, вычислители, сеть) в кластер и выделение мощностей для разных задач через виртуальный оркестратор. Наращивание мощности кластера производится путем добавления унифицированных блоков, что снижает расходы на хранение складских запасов и в целом увеличивает надежность системы. Ожидается, что в рамках такого подхода процесс заполнения ЦОДов может быть практически оптимальным.
- Гиперскалярный (Hyperscale) – наращивание мощности кластера путем добавления только компонентов того типа, мощность которых требуется нарастить. Отличие от традиционного ЦОДа (в котором все компоненты разделены) заключается в том, что все компоненты унифицированы и используются для всех задач без физического разделения. Сейчас это часто решения от одного вендора в рамках платформы гиперскалярной инфраструктуры.


Андрей Ивашов

Владельцам информационных систем придется действовать в условиях кадрового голода. Если раньше нам «дышали в спину» молодые специалисты, сейчас этого дыхания не ощущается. В плане эксплуатации надежда на новые системы автоматизации и предиктивное обслуживание.

Движение в сторону внедрения граничных вычислений и унифицирующих подходов потребует новых компетенций и других программных систем управления ЦОДом. Если раньше акцент делался на развитие специалистов и компетенций по типам систем, а также на создание инструментов мониторинга и управления для этих команд, то для распределенных и программно определяемых ЦОДов потребуется централизованная оркестрация как ИТ-, так и инженерных систем.

Самый базовый инженерный уровень – бесперебойное питание, распределение, охлаждение – меняется не столь революционно, как оберегаемая ими ИТ-начинка ЦОДов. И компетенции проектировщиков и специалистов по эксплуатации grey space подразумевают знания и опыт в области сложившихся практик. Вместе с тем этот уровень является базовым для эффективности и устойчивости всех целевых сервисов. Такие решения, как EcoStruxure IT, расширяют возможности мониторинга и обеспечива-

ют специалистов инструментами для своевременного реагирования, принятия повседневных решений и проведения модернизации на основе обработки больших данных и облачной аналитики.

Как показывает общемировая практика, масштабы и сложность ИТ-систем растут, а требования к их безопасности и устойчивости ужесточаются. Это подразумевает соответствующее развитие команд специалистов, сопровождающих эти системы. Риски различного рода, связанные с человеческим фактором, ведут к отказам. Человеческий фактор также влияет на то, что грамотно спроектированные системы годами не выходят на проектную загрузку, утилизируются неравномерно, происходят различные блокировки. Например, отсутствие средств моделирования загрузки ЦОДа может привести к тому, что не удастся реализовать современный проект с размещением высоконагруженного оборудования без инвестиций в систему охлаждения.

В корпоративных ЦОДах по-прежнему происходит разделение команд по принципу зон ответственности, а ресурсов – по подразделениям. Это затрудняет возврат инвестиций. В поисках простого подхода владельцы часто создают переразмеренные ЦОДы, иногда архаично разнося оборудование разных подразделений по разным стойкам. Мы часто видим незагруженные стойки и свободные площади при наличии резервов электропитания и охлаждения. Есть и менее очевидные случаи, когда требуются детальные измерения и аудит. Для аудита мы используем собственное решение StruxureWare, включающее средства измерения и ПО с наглядной визуализацией и отчетами. Даже однократное, пилотное использование решения позволяет обоснованно провести изменения, возвращающие ЦОД к эффективной работе или устраняющие риски отказов.

За последние несколько лет внедрение средств мониторинга, DCIM, CMMS, BIM помогло ряду заказчиков повысить эффективность использования технологических ресурсов и оптимизировать процессы. Но насколько централизованные решения могут закрыть потребности новых проектов цифровой экономики? Эти проекты обязательно будут использовать граничные вычисления, все перечисленные подходы с приставкой «гипер-», а сети будут географически расти и ветвиться. Управление инфраструктурой может столкнуться со сложностями, обусловленными дефицитом кадров, ростом числа контролируемых объектов и устройств, а также повышенными требованиями к безопасности и эффективности.

В этой ситуации мы как разработчики решений движемся вместе с технологическими трендами. Наше новое решение EcoStruxure IT Expert способно обеспечить максимальную эффективность мониторинга и достоверность аналитики. IT Expert представляет собой первый элемент облачной системы управления жизненным циклом для ЦОДов нового поколения. В основе решения – три компонента:

- шлюз мониторинга, обеспечивающий безопасный сбор технологической информации от оборудования любых вендоров;
- облачный сервис, обеспечивающий хранение данных, аналитику, отчеты и целый ряд новых инструментов;
- мобильное приложение для своевременных оповещений и непрерывного контроля систем.

> Очередной виток эволюции ИТ и появление гибридных архитектур требуют новых подходов к проектированию, развитию и управлению. Благодаря все более доступным облачным вычислениям программная часть приходит на помощь на всех этих этапах жизненного цикла.

Андрей Крюков

Облачный мониторинг в ближайшее время получит функции анализа для предиктивного обслуживания, а уже сейчас есть инструменты «бенчмаркинга» – сравнения состояния вашей системы с аналогичными, используемыми в сотнях других ЦОДов.

Мы надеемся, что эффективная и безопасная эксплуатация существующих и новых инфраструктур будет возможна в условиях кадрового голода и географического расширения. Специалисты «последней мили» получат достоверные данные и оповещения о состоянии их объектов, необходимых действиях и работах. Универсальная экспертиза при этом будет распределена между небольшой группой специалистов и средствами автоматизации, оснащенными инструментами машинного обучения и искусственного интеллекта. Команда, собственная или «на аутсорсе», сможет находиться удаленно и действовать в критических ситуациях или при проведении изменений в инфраструктуре.

Для эффективной работы такой модели потребуются профессионально спроектированный ЦОД с учетом будущего развития, наличие программы эксплуатации и развития и внедрение не только оперативного, но и прогнозного мониторинга на базе систем с самыми современными модулями анализа и статистики (на основе технологий Big Data и Machine Learning). Производителем и оператором данных систем должна быть компания с высоким уровнем экспертизы в области управления ЦОДами, способная гарантировать достижение высоких показателей эксплуатации и надежности.

Приглашаем партнеров и заказчиков ознакомиться и протестировать наше инновационное решение: https://ecostruxureit.com.

Мультиоблако: новый подход к построению ИТ-инфраструктуры

Александр Краснов, заместитель руководителя дирекции вычислительных комплексов, сервиса и аутсорсинга, «Инфосистемы Джет»

Не рискну строить предположения, насколько или когда инфраструктура российских компаний станет мультиоблачной. Но не сомневаюсь, что технологии и подходы, лежащие в основе этой концепции, значительно изменят ИТ-ландшафт уже в ближайшие пару лет.

Как и многие технологические тренды, термин «мультиоблако» пришел к нам с Запада. Так называют подход к созданию интегрированной инфраструктуры на базе нескольких облачных провайдеров. Мультиоблако обеспечивает высочайшие уровни доступности и масштабируемости, возможность разместить системы как можно ближе к пользователю, а также устранить технологическую зависимость от одного провайдера. Один из нашумевших примеров – Netflix, использующий одновременно AWS и GCP.

В отечественных реалиях мы чаще сталкиваемся с гибридным облаком как одним из подходов к созданию мультиоблака. Крупнейшие компании в России, которым важны высокие показатели отказоустойчивости и ручной доступ к «железу», сейчас предпочитают строить собственную облачную инфраструктуру. И если частное облако – это переход от «крафтовых» ИТ к конвейеру сервисов для бизнеса, то мультиоблако – это роботизированная фабрика, предоставляющая автоматический доступ к бизнес-приложениям.

Создание мультиоблака – сложный технический процесс. В мире еще не устоялась практика создания подобных ИТ-решений. Чтобы заставить гиперскейлеров работать вместе и использовать их как единое целое, нужно решить ряд задач. Среди них ключевые – адаптация приложений, обеспечение сетевой связности, доступности данных, повторяемости и единого управления.

Приложения

В идеальной ситуации на новую мультиоблачную инфраструктуру переносятся cloud native-приложения, соответствующие 12 критериям, сформулированным командой Heroku, а лучше – 15 критериям, описанным Кевином Хоффманом. При разработке таких приложений необходимо фокусироваться на возможностях облачных вычислений и особенностях виртуальной инфраструктуры.

Приложения, построенные в соответствии с устаревшими подходами, переносить в мультиоблако сложно и зачастую нецелесообразно. Но так как мы живем не в идеальном мире, приходится сталкиваться и с такими задачами.

Если абстрагироваться от вопросов разработки и сфокусироваться только на средах исполнения, необходимо обеспечить возможность развертывания всего приложения на основе декларативного описания конфигурации и исключить ручные операции.

Сетевая связность

Одна из сложнейших задач – добиться сетевой связности и доступности приложений как на внутренних площадках, так и между публичными облаками. Не многие крупные компании на российском рынке могут похвастаться сетью без пересечения адресных пространств. Чаще всего они сталкиваются с проблемой динамического выделения непересекающихся диапазонов внутренних адресов для неизвестного заранее количества подсетей.

В мультиоблачной архитектуре необходимо обеспечить доступность приложения как для внутренних, так и для внешних пользователей (если мы говорим о продуктивной среде) и партнеров (если мы говорим о большом количестве сред) вне зависимости от того, где приложение будет развернуто в следующий раз. А еще нужно обеспечить защиту, хотя бы на сетевом уровне, – и все в автоматическом режиме. Выбор технологии реализации программно определяемой сети передачи данных зависит от множества факторов и заслуживает отдельной статьи.

Доступность данных

Сегодня существуют три подхода к реализации доступности данных. Первый, пригодный только для гибридного облака – это репликация данных на уровне СХД или платформы виртуализации. Суть заключается в создании гибридной системы хранения и ее «растягивании» на каждое подключаемое облако. Такой же подход используется в классической инфраструктуре при создании ре-

зервного ЦОДа, и его главным ограничением является зависимость от решения вендора.

Второй подход – репликация резервных копий СУБД. Этот метод отлично подходит для случаев, когда допустима потеря данных, например, для тестовых сред. При этом для небольших объемов данных может использоваться инструментарий СУБД, а для значительных – отдельные системы резервного копирования.

Третий – это репликация данных на уровне СУБД. Несмотря на то что данные хранятся на уровне СХД, обрабатываются они на уровне СУБД, и с этого уровня мы можем поддерживать асинхронную репликацию. Случаи синхронной передачи данных необходимо рассматривать отдельно, так как в каждом конкретном приложении нужно искать баланс между производительностью на запись и сложностью логики записи самого приложения. Помимо данных СУБД, необходимо передавать информацию об остальных элементах системы.

Повторяемость

Обеспечить повторяемость – значит гарантировать запуск и работу приложения в объединенной мультиоблачной инфраструктуре на каждой площадке автоматически и без вмешательства человека. Если вы скажете, что это похоже на магию, то будете недалеки от истины.

На что важно обратить внимание: разные облака используют разные гипервизоры, и маловероятно, что виртуальная машина из внутреннего облака на одном гипервизоре будет работать в другом облаке. Поэтому самый надежный, но не самый простой путь – каждый раз разворачивать и подготавливать приложение с нуля. Для этого есть два подхода, и нужно выбрать не один, а правильное для конкретной компании и ее задач сочетание обоих.

Первый – использовать один из фреймворков автоматизации управления вычислительной инфраструктурой, например, Ansible, SaltStack, Chef и т.д. В этом случае нам как раз пригодится декларативное описание конфигурации, упоминавшееся выше.

Второй подход, сейчас активно набирающий популярность, заключается в «упаковке» отдельных сервисов в контейнеры. Прообраз технологии появился в Unix-системах больше 10 лет назад, но широко распространяться она стала только в последние годы. С одной стороны, возник спрос, а с другой – добавились некоторые вспомогательные технологии, которые позволяют использовать такой подход в промышленных масштабах. Программных продуктов для реализации этого подхода множество, самые популярные: Docker, rkt, PouchContainer.

Бинарный код и конфигурация контейнера содержатся в образе. Единожды собранный, он будет предсказуемо одинаково работать на всех платформах. Например, собранный и работающий на моем ноутбуке docker-образ будет точно так же работать в вашем ЦОДе или у гиперскейлера, была бы возможность выполнить команду docker run. Немаловажно, что если образ запустился на какой-либо платформе один раз, то он гарантированно запустится во все последующие – нужно только следить за доступностью ресурсов. В этом ключевой момент повторяемости. К сожалению, фреймворки автоматизации не могут гарантировать, что единожды успешно выполненный, например, playbook точно сработает в следующий раз.

> Приложения, построенные в соответствии с устаревшими подходами, переносить в мультиоблако сложно и зачастую нецелесообразно.

Следует понимать, что один контейнер – это еще не приложение, но процесс. Процессов, как и контейнеров, в мультиоблачной инфраструктуре будет много, они должны будут взаимодействовать как между собой, так и с конечным пользователем (через интернет или внутреннюю сеть). Для запуска приложения, состоящего из множества контейнеров, и управления им, нам потребуется оркестратор, например, Kubernetes, Mesos или Swarm. Он и будет разворачивать сразу несколько контейнеров, контролировать последовательность их запуска и отслеживать их доступность.

Единое управление

Последнее, но важное – объединение управления. В первую очередь необходимо автоматизировать процессы предоставления и сворачивания ресурсов сразу на нескольких платформах, мониторинга доступности, работоспособности приложений и использования ресурсов, не говоря уже о базовом обеспечении безопасности.

Скорее всего, вместе с автоматизацией придется поменять и сами процессы. Коллеги, уже прошедшие этот путь или большую его часть, в кулуарах конференций рассказывают, что это и есть самое сложное: с техникой справиться проще, чем с людьми, и готовых рецептов нет, но есть примеры. Как я говорил ранее, Netflix активно использует принцип мультиоблачности в построении ИТ-инфраструктуры. Для управления несколькими облаками компания разработала систему мультиоблачной доставки приложений – Spinnaker. Продукт с открытым исходным кодом поддерживает множество популярных сред развертывания, включая AWS, Azure, GCP, OpenStack и Kubernetes. ИКС

Rittal делится экспертизой с российскими заказчиками

Константин Бобылев

Центр ИТ-компетенций компании Rittal помогает российским клиентам в проектировании, внедрении и сопровождении комплексных решений для инженерной инфраструктуры ЦОДов, – говорит руководитель центра Константин Бобылев.

– Константин, в нашей стране мало знают о Центре ИТ-компетенций Rittal. Для чего он создан и почему в Литве?

– Появление центра было вызвано как экономическими причинами, так и организационными: не так легко найти слаженную команду высококвалифицированных специалистов. Литовская команда давно помогала коллегам, но официально Центр ИТ-компетенций Rittal открылся в Вильнюсе в январе 2016 г.

Центр обеспечивает поддержку полного спектра решений Rittal (ИТ-шкафы, энергоснабжение, охлаждение, мониторинг, вопросы безопасности) от выработки концептуального решения до сопровождения эксплуатации. Также наши сотрудники способны интегрировать продукты других поставщиков, например системы пожаротушения, и вписать их в общее решение.

Мы помогаем коллегам из Rittal осуществлять защиту проекта перед клиентом, подготавливаем документацию, презентации, участвуем в общении с заказчиком. В основном Центр ИТ-компетенций поддерживает партнеров, но иногда и клиентов.

Другой наш заказчик – сама компания Rittal. Далеко не везде подразделения компании имеют компетенции по всему спектру задач. Мы оказываем поддержку филиалам с ограниченным числом экспертов, например, в Египте, перспективной стране с быстро развивающимся рынком ЦОДов, где не хватает квалифицированных местных специалистов.

Кроме пресейла, центр помогает в реализации проектов. Наши сотрудники выезжают на пусконаладочные работы, тестируют инженерную инфраструктуру дата-центров. У нас есть сертифицированные специалисты по монтажу помещений безопасности и сейфов. Третьим направлением деятельности является организация обучений по тематике ЦОДов.

– Как давно центр работает с Россией?

– Российских коллег поддерживаем давно, но эта деятельность не освещалась широко в СМИ. Изначально была поставлена задача – поддерживать две ключевые страны: Финляндию и Россию. Помимо этих стран, работаем со всей Европой. У нас есть проекты в Африке и Азии, даже из Австралии иногда обращаются с просьбой о помощи по отдельным вопросам. Это не всегда выливается в поездки – просто помогаем коллегам в этих странах удаленно.

– А что центр предлагает российским партнерам?

– Помогаем с предпродажной подготовкой проектов и инженерных решений. Разрабатываем концепцию построения ЦОДа, создаем первичный проект и сопровождаем дальнейшее проектирование дата-центра. Сопровождаем реализацию проекта, поддерживаем пусконаладочные работы и процесс эксплуатации инженерных систем ЦОДов.

– Вы выполняете весь проект?

– География работы сотрудников центра очень широка, и потому сложно вести проекты ЦОДов с учетом регуляторной специфики каждой страны. Мы действуем как центр компетенций – создаем концепт, который реализуют, включая оформление документации, местные партнеры, способные согласовать проект с регуляторами и обеспечить получение всех необходимых подписей под схемами и чертежами. В основном это местные интеграторы. Центр разрабатывает концептуальное решение и специфицирует основное оборудование, но не детализирует проект до конечной спецификации.

– Как центр участвует в реализации проекта?

– Сотрудники центра выезжают к клиенту и участвуют в пусконаладочных работах. Например, запускают системы охлаждения, мониторинга, помогают коллегам установить системы управления ЦОДом, настроить DCIM.

– Как помогаете с эксплуатацией?

– Центр предоставляет консалтинговые услуги по проблемам, связанным с функционированием оборудования. Не всегда дело в поломке элемента, скажем, чиллера или кондиционера. Зачастую это вопросы системного характера, и нужно не диагностировать состояние конкретного узла, что по силами сервисной службе, а оптимизировать работу системы в целом.

– Какие еще услуги предлагает Центр ИТ-компетенций?

– У нас есть профессиональное программное обеспечение для моделирования тепловых процессов (Computational Fluid Dynamics, CFD). С его помощью исследуются как стационарные, так и различные переходные процессы, например то, как изменяется температура при выключении чиллера, оцениваются последствия отключения резервного элемента в системе. Это позволяет продемонстрировать заказчику, что предлагаемое решение будет соответствовать его требованиям.

Другое применение CFD-моделирования – оптимизация работы существующих дата-центров. На основе информации о геометрии ЦОДа и установленном в нем оборудовании с помощью моделирования можно проверить дата-центр на соответствие требованиям безопасности, оценить возможности размещения дополнительного оборудования, выяснить, как изменится картина при установке дополнительного активного оборудования в конкретных зонах. Наши сотрудники выезжают на объект, делают измерения, проводят валидацию модели (сверяют созданную трехмерную компьютерную модель с реальным объектом), проверяют установленное оборудование и режимы его эксплуатации, корректируют цифровую модель и проводят трехмерную симуляцию (исследование различных возможных ситуаций, например отключение кондиционера). А по итогам дают рекомендации заказчику.

Демонстрация ЦОДа российской группе клиентов в центре ИТ-компетенции

– Расскажите подробнее о программе обучения.

– В Вильнюсе работает демонстрационный ЦОД, в котором развернуты все необходимые элементы инфраструктуры – ИТ-шкафы, распределительные щиты, блоки розеток. В демонстрационном центре есть модульный источник бесперебойного питания, чиллер и системы мониторинга и DCIM. Наша команда занимается обучением с 2012 г., проводит занятия для новых сотрудников Rittal, партнеров и конечных пользователей. Программа обучения разнообразна, включает самые важные темы – от обзора стандартов и рекомендаций по построению инженерной инфраструктуры, систем холодоснабжения и энергоснабжения ЦОДов до примеров проектирования и эксплуатации. Иногда заказчики проходят обучение для того, чтобы понимать специфику работы купленного оборудования и порядок действий в нестандартных ситуациях. Это занятия не только по конкретному оборудованию, но и по инженерной инфраструктуре ЦОДа в целом. У наших специалистов есть сертификаты Uptime Institute и DataCenter Dynamics, полученными знаниями центр делится с клиентами.

– Приезжают ли обучаться в центр российские специалисты?

– Да, мы очень плотно сотрудничаем. В частности, российской была последняя группа – сотрудники крупного промышленного предприятия, взаимодействующего по внедряемому проекту с московским представительством Rittal. Как правило, запрос на обучение приходит от регионального представителя или конкретного заказчика, купившего наше оборудование.

– А с кем еще в мире сотрудничает центр?

– В Вильнюс приезжают даже из Южной Африки. Но наиболее тесное сотрудничество налажено с Германией и севером Европы: Финляндией, Швецией, Данией. Хорошие контакты с Чехией, Польшей, Италией и Испанией.

– Каковы конкурентные преимущества Центра ИТ-компетенций Rittal?

– Мы всегда выступали за комплексные решения. Соперничать на уровне шкафов и кондиционеров трудно, здесь высокая конкуренция. Заказчику нужны не отдельные элементы, а работающая инфраструктура в целом и сопутствующие знания ответственных сотрудников. Центр ИТ-компетенций отвечает за то, что дата-центр будет построен в соответствии с лучшими практиками и имеющимися в отрасли стандартами. Прибавив к этому обучение и поддержку, получите преимущества, привлекающие к нам заказчиков.

Российский рынок серверной виртуализации: тенденции и игроки

Николай Носов

Наряду с трендом перехода к облачным и мультиоблачным средам существует обратный тренд – перенос вычислений на площадки клиента. Игроки российского рынка серверной виртуализации отслеживают тенденции и ищут ниши в конкурентной борьбе.

Неэффективность использования вычислительных мощностей физических серверов привела к появлению виртуализации, созданию программными средствами виртуального представления ИТ-оборудования. Виртуализация повысила отдачу от использования техники, обеспечила легкость управления вычислительной средой и простоту масштабирования ее элементов.

Основные типы решений на рынке платформ серверной виртуализации: гипервизоры, используемые для создания виртуальных машин (VM); технологии виртуализации на основе операционных систем («контейнеры»); системы администрирования и управления виртуализацией серверов (миграция и автоматизация административных функций управления).

Рис. 1. Тенденции развития средств виртуализации

Тенденции развития средств виртуализации

Виртуальные машины, запускавшиеся на одном компьютере, появились еще в 70-х годах прошлого века, но их массовое использование началось совсем недавно. Первые реализации не вызывали особого восторга у пользователей – в виртуальной среде программы работали намного медленней. Но благодаря стремительному увеличению производительности компьютеров этот недостаток удалось сгладить, и решения пошли в массы.

Технологии серверной виртуализации лежат в основе облачных вычислений, популярность которых по-прежнему растет. В партнерстве с облачными провайдерами клиенты проводят цифровую трансформацию с меньшими рисками и затратами. Поэтому все больше компаний, особенно в сегменте малого и среднего бизнеса, отказываются от установки серверов в собственных помещениях, что негативно сказывается на динамике продаж гипервизоров.

При этом существует и противоположный тренд. Компании попробовали облачные вычисления, поняли, что они совсем не дешевы и не всегда эффективны, и стали возвращаться к использованию модели on-premise. Рынок ищет баланс между частными и публичными облаками, зачастую останавливаясь на гибридных моделях (рис. 1).

Популярность модели on-premise увеличивает и развитие гиперконвергентных решений, объединяющих вычислительные ресурсы, СХД, платформу виртуализации, средства развертывания программного и аппаратного обеспечения и управления его жизненным циклом. Благодаря таким системам пользователь получает преимущества облаков – гибкость и масштабируемость, но уже на своей площадке.

Необходимость приближения вычислительных мощностей к источнику данных и мини-

мизации задержек при их передаче привела к появлению граничных вычислений (Edge Computing), переносу вычислительной нагрузки на границу сети. По сути, создаются небольшие облачка, в которых для обеспечения гибкости инфраструктуры используется виртуализация. Над развитием этого направления активно работают как гиганты ИТ-индустрии (VMware, Microsoft), так и open source-сообщество OpenStack.

Как появление кинематографа не убило театр, так и новые технологии не приведут к отказу от классических облачных вычислений. Бизнесу нужны разные облака, вот почему более трети российских компаний планируют инвестиции в многооблачные среды, объединяющие лучшие предложения всевозможных облачных провайдеров. Переход от использования моновендорных решений виртуализации к экосистемам решений разных производителей – еще один тренд рынка.

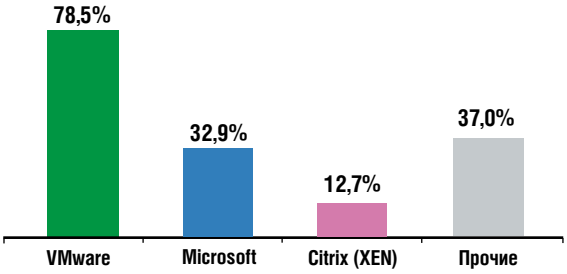
Управлять сложной облачной инфраструктурой нелегко, особенно в условиях роста популярности контейнерной виртуализации – еще одного тренда, связанного с широким использованием микросервисных архитектур и современных операционных моделей (Agile, DevOps). Инфраструктура должна быть максимально эффективной и автономной, требующей минимума ресурсов. Следующий тренд – переход к самовосстанавливающейся инфраструктуре на основе предиктивных моделей, технологий искусственного интеллекта (ИИ) и машинного обучения.

И последний, но очень важный тренд – повышение внимания к обеспечению безопасности платформ серверной виртуализации. Рассматриваются варианты защиты от внешних и внутренних угроз (в том числе с использованием методов ИИ) и от самих разработчиков аппаратных средств и программного обеспечения (отказ от поддержки ПО вследствие санкций, недокументированные возможности).

Кто двигает российский рынок?

Основные игроки на российском рынке платформ серверной виртуализации те же, что и в мире. Это VMware и Microsoft. Отличие только в разрыве между лидерами. Если в мире Microsoft нагоняет лидера, то в России отрыв по-прежнему велик.

Консалтинговое агентство iKS-Consulting в начале 2018 г. провело исследование российского рынка серверной виртуализации, в ходе которого оценивалась распространенность решений крупнейших игроков этого рынка. Было опрошено около 130 компаний. Респондентов просили сообщить, какой платформой серверной виртуализации они пользуются. Результаты опроса представлены на рис. 2.



Источник: опрос iKS-Consulting, 2018 г., респонденты могли называть несколько платформ виртуализации

Рис. 2. Использование платформ серверной виртуализации в России (процент опрошенных)

VMware была пионером на рынке серверной виртуализации. Сегодня в России много специалистов, имеющих опыт развертывания и эксплуатации ее решений, прежде всего – систем виртуализации на базе vSphere (гипервизор ESXi). Компания имеет разработки практически по всем наиболее перспективным направлениям развития рынка виртуализации.

«VMware сосредоточила усилия на четырех стратегических областях: модернизации центров обработки данных, интеграции публичных облаков, развитии цифрового рабочего пространства и трансформации информационной безопасности. Эти области для компании фокусные и в России, и глобально», – отмечает Артем Гениев, архитектор бизнес-решений VMware.

В погоне за лидером

У Microsoft есть свои козыри в борьбе за рынок. После того, как ее генеральным исполнительным директором был назначен Сатья Наделла, компания сконцентрировала внимание на развитии облачных сервисов и вполне в этом преуспела, в том числе в нашей стране. Опыт работы с Windows Server и on-premise-решениями виртуализации на гипервизоре Hyper-V помог российским пользователям в работе с облачными приложениями.

«У нас есть как программно-аппаратные комплекты (например, Microsoft Azure Stack) для построения облачных решений в периметре заказчика, так и публичное облако Microsoft Azure с внушительным набором сервисов, что позволяет создать оптимальные гибридные решения практически для любых запросов рынка. Это наше конкурентное преимущество перед другими компаниями в отрасли, которые способны или строить приватные облака, или предоставлять сервисы из своих глобальных дата-центров», – заявляет Андрей Выставкин, руководитель направления гибридных инфраструктур Microsoft.

Компания тоже предлагает широкий спектр решений: от базового продукта серверной виртуализации до гибридных облаков. В направлениях Edge Computing и IoT она, пожалуй, опере-

жает главного конкурента, по крайней мере на рынке SMB. Недостаток облачных решений – отсутствие в России дата-центров Microsoft – отчасти компенсируется гибридными системами.

Бронзовый Citrix

Третье место компании Citrix – результат, достигнутый в основном за счет получивших широкое распространение в нашей стране решений виртуализации десктопов (VDI). Сильной стороной компании является, в частности, работа с графикой. Так, XenServer, платформа для организации управления инфраструктурой серверов виртуализации на базе гипервизора Xen, обеспечивает виртуализацию графики разных производителей и выделение части реального графического ядра. А в рамках XenServer 7.4 компания совместно с NVIDIA предложила возможность переноса работающих машин с виртуальной графической картой с одного сервера на другой.

Ограниченные, по сравнению с лидером, возможности функционала ее решений для большинства заказчиков некритичны.

«*Многие заказчики предпочитают иметь для виртуальных десктопов одного поставщика. Поэтому выбирают XenServer, чтобы в случае нештатных ситуаций обращаться к Citrix, а не бегать между вендорами, пытаясь понять, кто же виноват в проблеме – гипервизор, брокер или виртуальная машина*», – поясняет официальный технический представитель компании Citrix в России Сергей Халяпин.

Незаметный Nutanix

Концентрация сил на наиболее выигрышном направлении – оптимальная стратегия для компаний, борющихся с двумя ИТ-гигантами рынка серверной виртуализации. Многие независимые эксперты отмечают систему виртуализации баз данных компании Nutanix, считая ее более быстрой и интересной в плане функционала, чем аналогичная система VMware vSAN. Используемый компанией гипервизор Acropolis создан на базе KVM, но сильно отличается от предшественника.

Из публичных кейсов можно выделить использование решения Nutanix в государственной системе взимания платы с большегрузных автомобилей «Платон», успешно функционирующей в России. Еще несколько лет назад компания была незаметна в информационном поле. Но в последнее время Nutanix стала более активной и полгода назад победила в тендере по выбору платформы виртуализации банка ВТБ-24.

«*В отличие от большинства других программных стеков виртуализации (как коммерческих, так и бесплатных), имплементирующих функционал на уровне ядра гипервизора, в решении Nutanix вся программная логика вынесена в изолированный виртуальный контроллер, что позволяет максимально обезопасить и облегчить ядро гипервизора. А размещение функционала в ядре (в том числе того, который не требуется в данный момент), по нашему мнению, вносит массу дополнительных рисков. Виртуальный контроллер Nutanix CVM работает на каждом узле (сервере) кластера вне зависимости от количества узлов. И подход себя оправдывает: мы сейчас одни из мировых лидеров и по скорости работы, и по безопасности для клиентов*», – с гордостью сообщает Максим Шапошников, директор по передовым технологиям Nutanix.

Российский Nutanix – «Росплатформа»

У решения Nutanix есть ограничения – для развертывания системы нужны сертифицированные серверы. С одной стороны, это хорошо – компания несет ответственность за нормальную работу решения на серверах Dell EMC и HPE, с другой стороны, сужает круг заказчиков.

Решение отечественной «Росплатформы», глава которой на конференциях часто позиционирует его как «российский Nutanix», более всеядно и, по утверждению представителей компании, может быть развернуто практически на любых серверах, допускающих установку ОС Linux.

«Росплатформа» – проект, инициированный компанией Parallels специально для программы импортозамещения. В основе ее платформы «Р-Виртуализация» лежат серверная виртуализация Virtuozzo (ранее Parallels Cloud Server), программно определяемое хранилище Virtuozzo Storage, оптимизированная линейка серверных операционных систем на базе Linux и виртуальные рабочие столы Parallels VDI. Компания делает ставку на гиперконвергентные системы и импортозамещение.

«*Своими конкурентными преимуществами «Росплатформа» считает создание гиперконвергентных систем на недорогом «железе» при максимальном использовании его ресурсов (процессоров, дисков, памяти), невысокую стоимость (заказчики, использующие классические, не гиперконвергентые решения, могут сэкономить на замене vSphere на «Р-Виртуализацию») и российское происхождение, устойчивое к санкциям*», – подчеркивает Владимир Рубанов, управляющий директор компании «Росплатформа».

Предложение из Поднебесной

Отношения с Западом продолжают ухудшаться, вводятся все новые санкции. Бизнес адаптируется к новым рискам и все чаще смотрит в сто-

рону Китая, который работает и на рынке серверной виртуализации.

Так, Huawei недавно запустила у нас в стране первое за пределами Китая публичное облако, работающее под ее брендом, открыла в Москве лабораторию OpenLab, которая выступает как связующее звено между российскими партнерами и китайской компанией. Huawei предлагает всю линейку инфраструктурных решений для цифровой трансформации. Компания занимает первое место в Китае на рынке частных облаков и объявила своей главной стратегической задачей попадание в число пяти облачных платформ, на вычислительной инфраструктуре которых будет идти цифровая трансформация мира.

Решения китайской компании имеют наименьшие санкционные риски среди остальных решений глобальных вендоров в сфере серверной виртуализации. При этом Huawei работает по всем направлениям развития рынка, предлагает решения для построения распределенного облачного ЦОДа FusionCloud (на базе OpenStack), где используется гипервизор Huawei FusionSphere (доработанный Xen), и платформу для пограничных вычислений Edge-Computing-IoT с интеграцией облачных вычислений и устройств (cloud-device integration).

Пока сложно говорить о существенном проникновении китайских решений серверной виртуализации на российский рынок, но потенциал у них, безусловно, есть.

Враг не пройдет

Специалисты обсуждают причины внезапной блокировки иракских ПВО во время операции «Буря в пустыне», СМИ – новый скандал, вызванный обвинением Китая в установке специальных микрочипов на материнские платы для американских серверов, а специалисты по информационной безопасности уже давно считают зарубежные аппаратные средства недоверенной средой. Однако «Эльбрусы» и «Байкалы» везде не установишь – дорого, и не для всех задач они подходят. Приходится использовать то, что предлагается на рынке.

В решениях зарубежных компаний для серверной виртуализации тоже могут скрываться недокументированные возможности. И безопасники оборонных отраслей, государственных и критически важных производств исходят из предположения, что они там есть. Если открытое ПО еще можно попытаться проверить, то в случае проприетарного придется верить на слово вендору, что не все могут себе позволить. Лучше положиться на сертификацию ФСТЭК.

По утверждениям представителей компании «Сервионика», разработанное ею решение РУСТЭК стало первой сертифицированной ФСТЭК российской платформой виртуализации со встроенным межсетевым экраном. В ней используется сертифицированный ФСТЭК гипервизор KVM со вспомогательной инфраструктурой (сеть, хранение данных). Сертифицированная система управления облачной инфраструктурой создана на базе OpenStack и включает собственные доработки «Сервионики». Подготовка платформы РУСТЭК к сертификации (включая испытания) заняла более двух лет. Платформа может быть развернута как в датацентре заказчика, так и в ЦОДе «ТрастИнфо», находящемся под управлением компании «Сервионика».

Российская компания Инновационный центр «Баррикады» изначально пошла по пути создания защищенного гипервизора, обеспечивающего разделение недоверенного оборудования и доверенных сервисов, выполняемых поверх среды виртуализации. Такой подход повышает безопасность системы в целом. Компания предлагает повысить защищенность систем за счет своего сертифицированного по российским требованиям безопасности решения виртуализации «Горизонт», построенного на базе KVM.

«*Мы имеем единственные в России сертификаты ФСТЭК на систему виртуализации как на средство безопасности, позволяющее на ее базе строить системы, которые связаны с обработкой секретных данных и персональных данных*», – уверяет Игорь Коптелов, заместитель генерального директора Инновационного центра «Баррикады».

■ ■ ■

Помимо перечисленных решений, на российском рынке присутствуют: Proxmox, система виртуализации с открытым исходным кодом, основанная на Debian GNU/Linux; платформа Red Hat Enterprise Virtualization, которая позиционируется как первая платформа виртуализации уровня предприятия, построенная на открытом исходном коде. Некоторые российские компании работают с Oracle VM Server (гипервизор XenServer).

Ряд компаний используют в инфраструктуре решения сразу нескольких производителей программного обеспечения для виртуализации одновременно. Но картину в целом это не меняет – с большим отрывом на рынке лидируют компании VMware и Microsoft, предлагающие решения по всему спектру направлений развития рынка виртуализации.

При дальнейшем ухудшении отношений с Западом и ужесточении режима санкций хорошие шансы на захват российского рынка получит компания Huawei. Конкуренцию составят российские компании, которые сейчас являются нишевыми игроками, ведущими борьбу за государственные организации и предприятия оборонного комплекса. ИКС

«Зеленый» ЦОД в Алабушево

В 2018 г. на рынок коммерческих ЦОДов России вышел новый игрок – один из крупнейших дата-центров GreenBush DC. Объект, рассчитанный на общую мощность 21 МВА и размещение 2280 стоек, расположен на территории «Алабушево» – особой экономической зоны города Москвы в административном округе Зеленоград.

На первом этапе реализации проекта в эксплуатацию вводится 6 машзалов на 660 стойко-мест (блок А2). На втором и третьем этапе – по 9 машинных залов на 810 стойко-мест на каждом этапе (блоки А1 и А3).

В машзалах возможно размещение как серверных шкафов стандартных размеров (до 48U), так и оборудования с нестандартными габаритами под требования заказчика. Мощность одного шкафа – до 20 кВт. Площади залов позволяют организовать выгородку клиентской зоны с организацией дополнительного уровня контроля физического доступа под управлением клиента.

На площадке размещено 6-этажное офисное здание и соединенное с ним здание ЦОДа, состоящее из 3 модулей по 5 этажей в каждом. Модульный принцип построения здания позволяет оптимизировать капитальные затраты, выделять необходимую площадь по мере роста заполняемости ЦОДа, а также роста потребностей клиентов.

GreenBushDC

ЦОД оснащен всеми необходимыми системами физической безопасности, включая систему охранной сигнализации, видеонаблюдения и многоуровневую систему контроля и управления доступом. Предусмотрено четыре уровня доступа в машзалы. Кроме того, территория имеет дополнительный, пятый уровень доступа – это охранный периметр ОЭЗ «Алабушево».

Инженерная инфраструктура дата-центра полностью соответствует требованиям TIER III по классификации Uptime Institute. Она построена с использованием самых современных, энергоэффективных технических решений. Так, для обеспечения бесперебойной подачи электропитания установлены динамические ИБП мощностью 1,67 МВА каждый.

Для охлаждения ИТ-оборудования в блоке А2, который вводится в эксплуатацию на первом этапе, использована классическая чиллерная схема. В других блоках (последующие этапы) предусмотрена установка систем адиабатического охлаждения.

http://greendc.ru

Вычисления на границе

Сергей Орлов, независимый эксперт

Сегодня наряду с централизацией вычислений в ЦОДах наблюдается тенденция к децентрализации, к обработке и хранению данных там, где они генерируются и используются. Вычисления и аналитика смещаются к границе сети – месту сбора больших объемов данных.

По мнению экспертов Gartner, к 2020 г. порядка 50% всех данных, генерируемых предприятиями, будут обрабатываться за пределами традиционного ЦОДа или облачной среды. Сегодня этот показатель составляет лишь 10%. По оценкам, к 2020 г. в такой архитектуре будут работать 5,6 млрд устройств интернета вещей (IoT). Объемы продуцируемых устройствами данных исчисляются терабайтами, и нередко интерпретировать их нужно в реальном времени.

С распространением приложений IoT, уменьшением допустимой величины задержки и ростом требований к автономии и безопасности становится критически важным физически приблизить вычисления к месту создания данных. Производители серверов не оставляют без внимания эту тенденцию и предлагают решения, отвечающие специфическим запросам граничных (или периферийных) вычислений.

Некоторые системы периферийных вычислений специально разрабатываются для IoT. Таковы, например, HPE Edgeline – системы промышленного класса для периферии сети, способные работать практически в любой среде (рис. 1). Подчас от подобных систем требуется высокая производительность для получения данных в режиме реального времени и решения аналитических задач, способность получать от IoT-устройств данные и обмениваться ими на высоких скоростях, оптимизировать доступ к ним, снизить затраты и риски, связанные с передачей данных по сети.

Разнообразие требований и задач породило столь же широкий спектр «граничных» систем – от интеллектуальных устройств со встроенными функциями ПК (все более производительных и «умных», однако известных уже не одно десятилетие) и IoT-шлюзов до серверов, гиперконвергентных решений и микроЦОДов с мощными вычислительными и аналитическими возможностями.

Задачи периферии

Периферийные вычислительные системы представляют собой распределенную ИТ-архитектуру, в которой данные обрабатываются самим периферийным устройством или локальным сервером. Менять традиционную архитектуру заставляет как развитие приложений IoT, так и быстрый рост объемов данных, передаваемых в мобильных сетях.

В случае граничных вычислений датчики и подключенные устройства передают данные ближайшему периферийному вычислительному устройству, а не отправляют их в облако или удаленный ЦОД. В результате приложения или устройства могут реагировать на новые данные без задержки, практически сразу после их создания.

Кроме того, иногда слишком дорого переносить все данные в ЦОД с периферийных площадок, где размещены устройства, поскольку для этого требуется значительная пропускная способность. Периферийные вычисления дают возможность эффективно обрабатывать большие объемы данных рядом с их источником, а в ЦОД или в облако передавать только те данные, которые требуют дальнейшего анализа или долгосрочного хранения. Это помогает снизить загрузку каналов передачи данных, требования к полосе пропускания сети и риски при работе с конфиденциальной информацией. Ограничение

Рис. 1. IoT-устройства HPE Edgeline

Рис. 2. Шлюзы Dell Edge Gateway серии 3000

передачи информации по сети уменьшает ее подверженность атакам хакеров. Появляется возможность применения различных удаленных приложений.

Одно из таких приложений – системы искусственного интеллекта. Так, по данным опроса HPE, промышленные предприятия будут внедрять гибридную архитектуру: инфраструктура ИИ будет распределена равномерно между периферийными объектами, ЦОДами и облачными хранилищами. Такой подход позволит обрабатывать данные на периферийных устройствах в режиме реального времени, а также проверять данные из разных источников одновременно с обучением моделей.

Поскольку нет необходимости перемещать большие объемы данных между географически разнесенными площадками, можно сократить затраты на создание сетей. Еще одна область применения периферийных вычислений – мониторинг сетевой безопасности, эффективное предотвращение вирусных атак или распространения вредоносного ПО.

Граница сети как передний край технологических инноваций

Периферийные вычисления привлекают сегодня внимание практически всех крупных (и не очень) поставщиков серверных платформ, которые спешат представить свои новинки данного сегмента серверного рынка.

По сути, периферийные серверы играют роль шлюзов между оконечными устройствами и ЦОДом или облаком. Некоторые из них так и называются. Пример – шлюзы Dell Edge Gateway серии 3000, которые можно применять в качестве встроенных решений в системах промышленной автоматизации, в энергетике, на транспорте (рис. 2). Интересна «начинка» этих устройств. В шлюзах установлены процессор Intel Atom, ОЗУ 2 Гбайт и хранилище eMMC 8 Гбайт. Есть интерфейсы Ethernet, USB, Wi-Fi, Bluetooth LE, поддержка 3G или 4G LTE. Также имеется цифровой модуль GPS, акселерометры и датчики атмосферного давления, поддержка PoE. Устройства могут работать при температуре от –30°C до +70°C. Каждая модель (а всего их три) сконфигурирована для конкретного целевого рынка. Тем не менее шлюзы серии 3000 достаточно универсальны, а потому подходят для разных отраслей и сценариев использования.

Гиперконвергентные инфраструктуры, признанные одной из наиболее перспективных технологий для создания частных и гибридных облаков, теперь выходят на границу сети. Один из примеров – Cisco HyperFlex, оптимизированное для периметра сети решение, предназначенное для распределенных организаций и сетей филиалов. Система представляет собой трехузловой кластер, настроенный для использования существующей сети, простой в развертывании и управлении.

Рис. 3. МикроЦОДы Dell EMC micro MDC

Его задача – эффективно обслуживать сотрудников во фронт-офисах. Вычислительная инфраструктура на периметре сети должна быть мощной, надежной, способной работать непрерывно и независимо от корпоративного датацентра, даже в случае сбоя, считают в Cisco. Благодаря высокой надежности ее развернутые на периметре сети системы смогут обеспечить доступность приложений и данных при самых разных сценариях отказов.

Однако самые «тяжеловесные» и мощные периферийные системы – это микроЦОДы. Например, микроЦОДы Dell EMC micro MDC на базе серверов x86 (рис. 3) предназначены для того, чтобы приблизить обработку данных к пользователю. Поставляются они в виде предварительно интегрированного, готового решения и ориентированы в основном на провайдеров и телеком. Размещать их можно как в помещении, так и на улице. Dell EMC micro MDC управляется с помощью программного обеспечения MDCi. Операторы могут администрировать и управлять несколькими MDC с помощью единого портала. МикроЦОД содержит от 0,5 до 3 стоек с ИТ-оборудованием, встроенную систему охлаждения и ИБП. Есть варианты с малой, средней и высокой плотностью размещения оборудования.

Рис. 4. МикроЦОД Rittal Edge Data Center

Рис. 5.
Три модели микроЦОДов от Schneider Electric

Сходное законченное решение предлагает и Rittal, оно так и называется – Edge Data Center (рис. 4). Такой микроЦОД включает до восьми ИТ-стоек и содержит все необходимое для размещения и работы активного ИТ-оборудования: стойки, системы холодоснабжения, бесперебойного питания, пожаротушения, мониторинга и пр. Если заказчику требуется максимально безопасное и надежное решение, то Rittal может поместить Edge Data Center в сейфовую оболочку.

Компания Schneider Electric разработала свой микроЦОД совместно с партнерами – Cisco и Nutanix. Эта гиперконвергентная платформа выпускается в трех вариантах (рис. 5) для разных целевых рынков – ритейл, финансовая отрасль, госсектор.

Все эти решения появились в 2017 г. В заключение – несколько слов о последних новинках 2018 г. Характерно, что даже Microsoft в сентябре 2018 г. представила Azure Data Box Edge – специальный сервер периферийных вычислений на процессорах FPGA для приложений искусственного интеллекта с последующей обработкой данных в облаке Azure (рис. 6). Он работает с программным обеспечением с открытым исходным кодом, так что сторонние разработчики могут создавать собственные решения. Как сообщает Microsoft, устройства Azure Data Box позволяют быстро, недорого и надежно передавать сотни терабайт данных в облако Azure.

Рис. 6.
Сетевые устройства Microsoft Azure Data Box

Intel и Alibaba запустили недавно плод совместной работы – Joint Edge Computing Platform. В этой платформе с открытой архитектурой программные, аппаратные технологии Intel и ее разработки в области ИИ интегрированы с IoT-продуктами Alibaba Cloud. Искусственный интеллект используется для того, чтобы преобразовывать получаемые на границе сети данные в аналитические рекомендации для бизнеса. Платформу можно адаптировать для конкретных задач, например, для интеллектуальных зданий или производств.

Решать задачи ИИ на периферии под силу не только серверам с процессорами Intel или AMD. Недавно анонсированная архитектура ARM Cortex-A76, как заявлено, позволяет вчетверо быстрее прежней версии выполнять алгоритмы ИИ и машинного обучения. Проект ARM Project Trillium Machine Learning обещает еще большие достижения.

■ ■ ■

Периферийные вычисления органично дополняют облачные. Периферийное устройство по существу является специализированным или многофункциональным сервером вне центра обработки данных и представляет собой интерфейс к вышестоящим системам, с одной стороны, и к источникам данных – с другой.

Производители таких решений, как правило, используют свои наработки в области традиционных вычислений (серверы, ПК) и «кастомизируют» под решаемые задачи, применяют в качестве элементов или платформ периферийных вычислений традиционные серверы или серверные модули. В 2016 г. был создан Консорциум периферийных вычислений (Edge Computing Consortium), в который сейчас входят свыше 180 участников.

По прогнозу Gartner, к 2021 г. 40% предприятий в мире разработают полномасштабные стратегии периферийных вычислений, в то время как на конец 2017 г. такие стратегии были лишь у 1% организаций. Вот почему вендоры торопятся занять перспективную нишу. Очевидно, что в ближайшее время мы увидим много интересных новинок, а компании, реализующие возможности граничных вычислений, смогут воспользоваться преимуществами развития новых направлений бизнеса. В ближайшие пять лет этот рынок будет активно формироваться, появятся платформы и готовые решения, ориентированные на различные задачи и отрасли. Основными драйверами его развития станут различные сценарии IoT и переход на сети 5G. ИКС

Транспортные сети 5G
Когда ответы неочевидны

Развертывание коммерческой сети 5G окажет определяющее влияние на развитие транспортной сети 5G RAN, и операторы понимают важность расширения своей экосистемы производителей для получения оптимальных технических решений и коммерческих условий.

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

Разноплановые аспекты комплексной задачи

Нет никаких сомнений в важности скорейшего коммерческого запуска сетей 5G. Для вендоров это возможность окупить инвестиции в разработку и увеличить объемы продаж, для операторов – повышение рентабельности бизнеса за счет использования более эффективных технологий и получение новых источников прибыли при расширении портфеля услуг.

Однако по мере приближения коммерческого внедрения 5G у операторов остается все меньше времени для принятия решений о развитии своих транспортных сетей. Эти сети должны стать основой высокоскоростных, предполагающих низкие сетевые задержки услуг, которые операторы планируют запускать и монетизировать.

Стратегическое решение практически всегда является комплексной задачей. Разработка оптимальной стратегии развития транспортных сетей 5G также предполагает разноплановые вопросы, ответы на которые до сих пор неочевидны:

- Какое место отводится в транспортной сети 5G RAN (Radio Access Network) радиорелейным технологиям?
  Понятно, что оптоволоконные системы способны максимально удовлетворить требованиям к пропускной способности и минимальным сетевым задержкам. В каких типовых решениях 5G RAN наиболее эффективными будут радиорелейные транспортные каналы?
- Какие приложения будут наиболее востребованы на рынке после запуска коммерческих сетей 5G и какие в наибольшей степени затронут транспортные сети?
  Инвестиции в строительство транспортных сетей – существенная часть затрат оператора на создание сетей 5G. Поэтому использоваться они должны максимально эффективно для высокой коммерческой результативности внедрения новой мобильной технологии.
- Могут ли – и если могут, то в какой степени – пакетные технологии взять на себя нагрузку на транспортную сеть, которую будет создавать трафик, генерируемый новыми приложениями?
  В настоящее время все функции цифровой обработки сконцентрированы в BBU (Baseband Unit), а по интерфейсу CPRI (Common Public Radio Interface) между RRU (Remote Radio Unit) и BBU передается модулированный радиосигнал в оцифрованном виде (рис. 1а). При этом скорость на CPRI-интерфейсе постоянна. Необходимость обработки более широкополосного сигнала и минимизация сетевых задержек в 5G обусловили новое функциональное деление между узлами радиосети RAN (рис. 1б). Трафик новых интерфейсов eCPRI (enhanced CPRI) и F1 в отличие от CPRI является пакетным, и его скорость зависит от загрузки сети абонентским трафиком. Очевидно, что агрегация такого трафика может оптимизировать размер требуемых транспортных ресурсов.
- Кто будет поставлять транспортные решения 5G RAN операторам?

Последний вопрос вызывает на рынке, пожалуй, наибольший интерес.

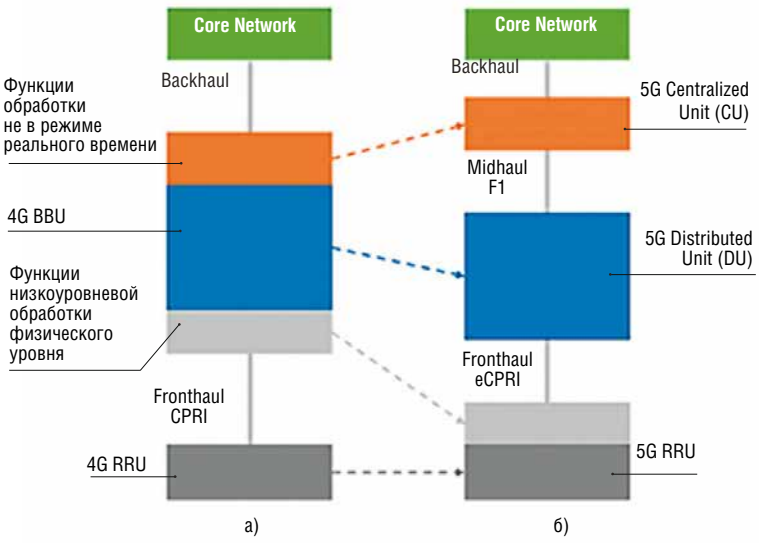


Рис. 1. Функциональное деление между узлами RAN: а) в сети 4G б) в сети 5G

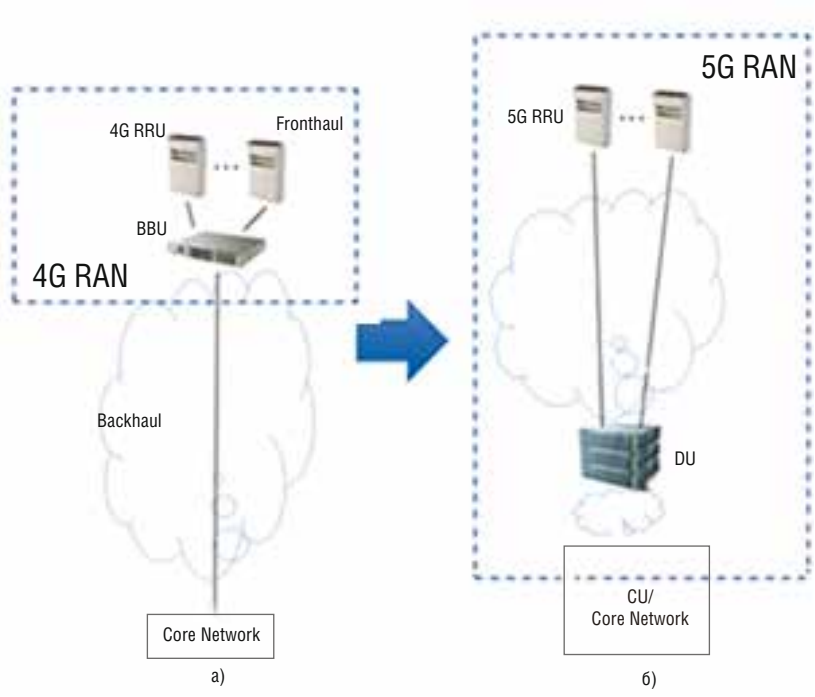


Рис. 2. Архитектура радиосети RAN:
а) распределенная архитектура 4G RAN
б) централизованная архитектура 5G RAN

Деликатный вопрос выбора поставщиков

Основной путь развития мобильных сетей 4G – увеличение количества базовых станций (БС), каждая из которых обслуживает свою территорию автономно. Поэтому сейчас наиболее распространенной является так называемая распределенная архитектура RAN, в которой устройства БС (BBU и RRU) располагаются на одной площадке. При этом сеть 4G состоит из радиодомена RAN, транспортного домена Backhaul и домена опорной сети Core Network (рис. 2а).

Термин Fronthaul, обозначающий транспортный домен между RRU и BBU, до настоящего времени использовался редко, поскольку часто рассматривался как составная часть базовой станции и, как правило, поставлялся производителями в качестве сопутствующего оборудования БС.

Как полагает большинство экспертов, для 5G оптимальна централизованная архитектура RAN (рис. 2б), при которой решения транспортной сети во многом определяются трафиком Fronthaul. Это связано как с более жесткими функциональными требованиями к транспортной сети (максимальной сетевой задержкой, допустимым уровнем джиттера), так и доминирующим объемом этого трафика (до 25 Гбит/с на RRU) при одновременном возрастании требований к экономической эффективности самих решений и максимальному использованию потенциала существующих линий связи.

Возможность стандартизации eCPRI и, следовательно, приобретения RRU, DU, CU у разных производителей активно прорабатывается с участием крупнейших мобильных операторов (Deutsche Telekom, AT&T, Verizon и т.д.) в рамках различных международных инициатив (xRAN, Open RAN и т.п.). К настоящему времени опубликована первая версия спецификации интерфейса eCPRI.

Интерес к возможным поставщикам транспортных решений 5G RAN связан с тем, что осознание операторами важности демонополизации рынка поставщиков RAN не ограничивается выбором различных поставщиков узлов базовых станций, а распространяется и на транспортную сеть RAN.

Это предположение подтверждается исследованием, которое провело независимое телекомиздание Light Reading. Согласно опросу, выполненному летом этого года исследовательским подразделением Light Reading (оно называется Heavy Reading), большинство операторов хотя и считают традиционных поставщиков радиооборудования предпочтительными вендорами для транспортных сетей 5G RAN, финального выбора поставщиков еще не сделали и планируют пригласить новых поставщиков. Главные причины такой установки – стремление к усилению ценовой конкуренции и сомнения в том, что единственный поставщик сможет предложить оптимальные транспортные решения для всего разнообразия существующей сетевой инфраструктуры и топологии.

Данный подход имеет под собой серьезное основание, поскольку, согласно тому же исследованию, практически все опрошенные операторы считают, что хорошо представляют себе то влияние, которое окажет внедрение 5G на стратегию развития транспортной сети (рис. 3).

Таким образом, в условиях приближения коммерческого внедрения 5G операторы хорошо представляют себе стоящие перед ними цели построения транспортной сети 5G RAN, способы их наилучшего достижения, а также осознают важность расширения своей экосистемы производителей для получения оптимальных технических решений и коммерческих условий. ИКС

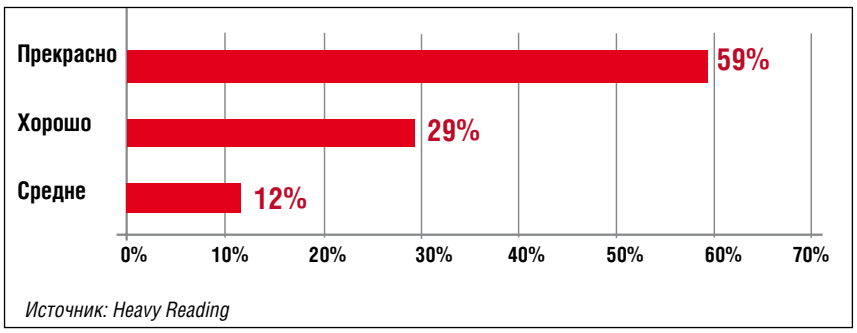


Рис. 3. Мнения операторов о понимании ими влияния 5G на стратегию строительства транспортной сети

Новые кабельные решения для ЦОДов

Новые технологии для кабельных систем во многом ориентируются на дата-центры и существенно увеличивают скорости передачи данных.

Николай Носов

Стоимость СКС составляет 3% стоимости ЦОДа, однако кабельные соединения, как сообщил на организованной «ИКС-Медиа» конференции «ЦОД-2018» Сергей Горюнов, менеджер по развитию продаж компании Molex MPN Structured Cabling, являются причиной 70% инцидентов. А инцидент в ЦОДе – это потеря денег, репутации и доверия клиентов.

Волшебное слово «быстро»!

Вложения в кабельную систему – долгосрочные, ведь средний срок ее эксплуатации составляет 10–15 лет. Поэтому при проектировании СКС следует учитывать перспективу стремительного роста объема передаваемых данных и требований к скорости передачи по каналам связи. Если в офисных СКС по-прежнему встречаются каналы 10 Мбит/с, то в ЦОДах уже используются каналы с пропускной способностью 100 Гбит/с. И это не предел. В декабре 2017 г. официально принят новый стандарт IEEE 802.3bs, предусматривающий увеличение скорости канала до 200 и 400 Гбит/с (см. таблицу).

Оборудование, отвечающее стандарту IEEE 802.3bs, уже появляется на рынке. Так, в 2018 г. упомянутая Molex начала производить поддерживающие новые стандарты коннекторы высокой плотности, а Mellanox Technolgies, по заявлению системного инженера этой компании Александра Петровского, планирует в следующем году выпустить коммутаторы с портами 400 Гбит/с.

Ethernet для СХД

Одна из сфер применения нового стандарта – Ethernet-фабрики для систем хранения данных (Ethernet Storage Fabric, ESF). Раньше СХД рассматривалась как некая проприетарная система с набором дисков, подключенная к сети хранения данных. Ее было сложно обслуживать и дорого масштабировать. Сейчас, особенно в облачных инфраструктурах, используются программно определяемые хранилища. Для их создания обычные серверы с большим количеством дисков масштабируются горизонтально в виде одного большого пула хранения, а программные решения формируют из них общий кластер. Подключаются серверы друг к другу с помощью высокоскоростной сети. Для этих целей теперь может использоваться технология Ethernet, которая значительно выигрывает в скорости у Fibre Chanel, способной обеспечить производительность не более 32 Гбит/с.

Сеть Ethernet-фабрики для хранилища строится в топологии Leaf-Spine (рис. 1). К коммутаторам уровня Leaf подключаются серверы (узлы хранения). Хранилище масштабируется стойками – от одной до тысячи и более. В каждую стойку устанавливаются по два коммутатора, которые подключаются к вышестоящей фабрике. Для подключения служат каналы 40 и 100 Гбит/с, а с внедрением нового стандарта скорости вырастут еще больше. ESF поддерживает широкий набор СХД-протоколов и приложений: iSCSI/iSER, FS/NFSoRDMA, CIFS/SMB Direct, NVMeOF, Ceph, HDFS, Lustre/GPFS/GlusterFS.

Витая пара для ЦОДов

Новации в кабельных системах для ЦОДов коснулись не только оптики, но и электропроводных решений. Для связи серверов с коммута-

Спецификации стандарта IEEE 802.3bs

Спецификация	Расстояние, м	Тип волокна*	Примечание
400GBASE-SR16	100	MM	По 16 волокон на прием и передачу
400GBASE-DR4	500	SM	Четыре параллельных волокна в обоих направлениях, 100 Гбит/с на одно волокно
400GBASE-FR8	2000	SM	WDM (два волокна, одно на прием, другое на передачу)
400GBASE-LR8	10000	SM	То же
200GBASE-DR4	500	SM	Четыре параллельных волокна в обоих направлениях
200GBASE-FR4	2000	SM	WDM (два волокна, одно на прием, другое на передачу)
200GBASE-LR4	10000	SM	То же
***SM – одномодовое, MM – многомодовое**			

Источник: IEEE

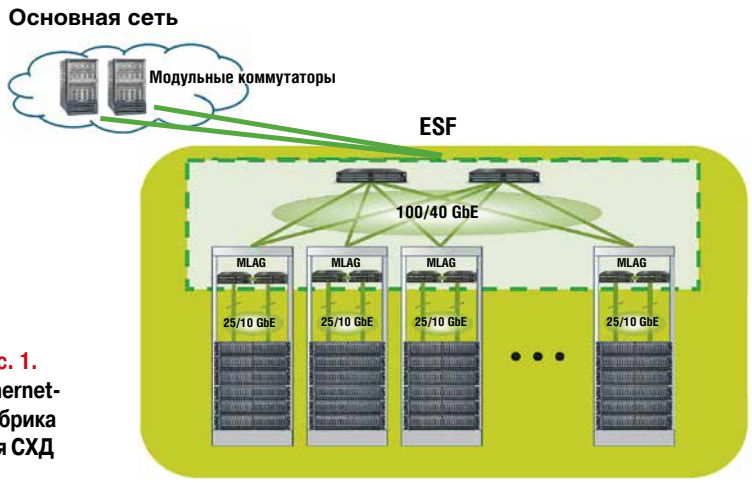


Рис. 1. Ethernet-фабрика для СХД

Источник: Mellanox Technologies

торами в дата-центрах появились кабели восьмой категории (Cat8) на медной витой паре, поддерживающие скорость 25 и 40 Гбит/с. Принятие стандарта категории 8 заняло почти 10 лет: его предшественник, востребованный на практике стандарт категории 6a, был принят еще в 2008 г. Кабели Cat8 отличаются от предшественников частотой (до 2 ГГц, что в четыре раза выше, чем у 6a), длиной тракта (не более 30 м, в то время как у 6a – 100 м), числом коннекторов (не более двух – кросс-коннект запрещен), конструкцией кабеля (каждая витая пара в фольге, все вместе в металлической оплетке, а экранирование требует заземления) и коннекторов (существуют две модификации – 8.1 (RG-45) и 8.2 (Tera, GG45, ARJ)).

Новый кабель слишком короткий для прокладки в офисных зданиях, но отлично подходит для организации внутрирядной связи в дата-центрах. Ограничение длины кабелей категории 8 тридцатью метрами не случайно. Таким образом, пояснил директор по продажам компании Leviton Сергей Логинов, достигается оптимальный баланс между мощностью трансиверов и дальностью передачи сигнала, позволяющий снизить энергопотребление и соответствующие операционные издержки.

С помощью кабелей категории 8 для соединения стоек в машзалах ЦОДов можно реализовать несколько типов архитектур (рис. 2) – End-of-Row (коммутаторы располагаются в конце ряда стоек), Middle-of-Row (в середине) и Top-of-Rack (коммутаторы размещаются вверху стоек с ИТ-оборудованием).

End-of-Row (EoR) и Middle-of-Row (MoR) предполагают классический подход к построению структурированной кабельной системы, при котором коммутационные шнуры соединяют оборудование через коммутационные панели.

При часто используемой в дата-центрах архитектуре Top-of-Rack (ToR) ИТ-оборудование подключается напрямую к расположенным вверху стойки коммутаторам. У каждого такого коммутатора есть оптические порты, соединенные с коммутаторами уровня агрегации. Такая схема не является классической для структурированной кабельной системы, но для 8-й категории просто подключение коммутационным шнуром уже может рассматриваться как СКС.

Кабели категории 8 дешевле, чем оптические, обеспечивают обратную совместимость с кабелями категории 6 (разные порты одного коммутатора могут поддерживать разные скорости), так что при их использовании заказчик получает универсальную инфраструктуру, способную работать на скоростях от 1 до 40 Гбит/с.

Cat8 – идеальный вариант для малых и средних ЦОДов, в машинных залах которых в одном ряду размещается не более 30 стоек. В крупных ЦОДах, где стоек в рядах более 30 и требуются скорости выше 40 Гбит/с, следует применять оптоволокно.

Рис. 2. Варианты подключения стоек с использованием Cat8

Источник: Leviton

С. Логинов призывает правильно проектировать кабельную систему на основе кабелей категории 6a и использовать архитектуру ToR, тогда для перехода на стандарт Cat8 будет достаточно заменить коммутационные шнуры. При выборе между EoR и MoR следует остановиться на MoR – это позволит организовать более длинный ряд стоек. Кроме того, предпочтительнее использовать экранированный кабель категории 6a, поскольку наличие заземления облегчит переход на Cat8. ИКС

СКС категории 8 и 25G Ethernet

Линии связи в ЦОДах, построенные на основе СКС категории 8 в сочетании с сетевыми интерфейсами 25G Ethernet, объединяют в себе достоинства электропроводных решений с высокими скоростными характеристиками волоконно-оптической техники.

Андрей Семенов, профессор, МТУСИ

Хотя профильные стандарты допускают создание физического уровня телекоммуникационной инфраструктуры дата-центров на основе как симметричной электропроводной, так и волоконно-оптической техники, проблема выбора типа элементной базы СКС для средних и крупных ЦОДов до последнего времени не стояла: промышленность серийно не производила электропроводную технику, изначально рассчитанную на передачу данных со скоростью 40 Гбит/с и выше или адаптированную к ней. Положение радикально поменялось после стандартизации элементной базы категории 8.

Электропроводные решения имеют целый ряд преимуществ по сравнению с волоконно-оптическими:

- ✓ за счет отсутствия дополнительного преобразования сигнала не только уменьшается задержка, но и в 1,5–2 раза снижается стоимость 40-гигабитного сетевого интерфейса;
- ✓ на дальности примерно до 35–40 м обеспечивается существенный выигрыш в потребляемой мощности (ключевой параметр для ЦОДа);
- ✓ заметно ослабляются требования к качеству монтажа и сохраняется возможность формирования линий в полевых условиях «по месту»;
- ✓ упрощается эксплуатационное обслуживание и уменьшаются трудозатраты на него.

Последнее связано с эффектом взаимной самоочистки контактной группы вилки и розетки модульного разъема в момент создания соединения, который обусловлен использованной схемой контактной шины. Этот эффект позволяет не контролировать дополнительно состояние взаимодействующих между собой электрически активных поверхностей.

Вместе с тем в силу сложности технологии при построении волоконно-оптических трактов для скоростей 40 Гбит/с и выше доминирующее положение занимает претерминированная техника заводского изготовления. При всех ее достоинствах всегда следует помнить о том, что ее применение существенно ужесточает требования к качеству проработки проектных решений.

Возможность передачи 100-гигабитного информационного потока по симметричной линии на расстояние 100 м с качеством, достаточным для коммерческого использования, была экспериментально продемонстрирована еще в конце 2000-х гг. Тем не менее этот потенциал до настоящего времени не востребован. Это обусловлено следующими факторами:

- потеря преимуществ в энергетической эффективности на длинных (по меркам ЦОДов) линиях;
- отсутствие технического задела в части достижения скоростей свыше 100 Гбит/с;
- неудовлетворительные массогабаритные параметры электропроводных кабельных изделий;
- отсутствие широкой потребности в обеспечении дистанционного питания по технологии PoE для маломощных терминальных устройств.

Таким образом, область применения электропроводной техники категории 8 определяется сравнительно невысокими быстродействием и дальностью и фактически ограничивается нижним уровнем структурированной проводки, включая внутрирядные связи в машинных залах ЦОДов.

Почему 25G Ethernet

В отличие от сетей связи общего пользования, в которых у каждого следующего поколения аппаратуры скорость передачи данных в четыре раза выше, чем у предыдущего, в сетевых интерфейсах Ethernet локальных сетей было принято 10-кратное наращивание скорости. Такая стратегия использовалась свыше двух десятков лет, и отказались от нее только при выходе за границы 10 Гбит/с. Побудили к

Рис. 1. Уровни требований различных нормативных документов

отказу от удобного и эффектного с маркетинговой точки зрения традиционного подхода следующие обстоятельства:

- невозможность простого увеличения количества субканалов при параллельной передаче, общепринятой на высоких скоростях информационного обмена, в медножильных сетевых интерфейсах из-за наличия в стандартном горизонтальном кабеле СКС четырех витых пар;
- сложность повышения тактовой частоты из-за ограниченного быстродействия современной микроэлектронной элементной базы;
- возможность снижения затрат и продолжительности НИОКР за счет использования наработок в сфере схемных решений для сетей связи общего пользования.

Кроме того, введение промежуточных значений скоростей оказалось выгодным для некоторых видов новых приложений. Так, стандартизация скоростей 2,5 и 5 Гбит/с позволяет заметно улучшить технико-экономические параметры сетей Wi-Fi. В сочетании с увеличенным быстродействием это должно способствовать более широкому использованию популярной беспроводной техники.

В случае 25G Ethernet новая скоростная градация была введена сразу же за созданием 40-гигабитных интерфейсов. Снижение скорости передачи в 1,5 раза означает удешевление техники, привлекательное с учетом количества линий связи в ЦОДах. А повышение скорости в 2,5 раза по сравнению с устройствами 10G Ethernet позволяет использовать новую элементную базу сначала на магистральных участках сети, а по мере роста скоростей информационных потоков постепенно переводить ее на более низкие уровни. Фактически это означает примерное удвоение периода «моральной молодости» техники.

Кроме того, скорость 25 Гбит/с лучше соответствует потребностям подсистемы массовой памяти, которая из-за особенностей реализации требует несколько меньшего быстродействия каналов связи.

Стремление к улучшению качественных показателей функционирования ЦОДов привело к расширению использования в информационной инфраструктуре машинных залов так называемых плоских структур с уменьшенным количеством ступеней иерархии и высокой связностью отдельных узлов. Сокращение времени задержки сопровождается ростом средней протяженности тракта и нарушением того распределения их длин, на которое в свое время ориентировались разработчики 40G Ethernet. В этой ситуации техника 25G Ethernet, имеющая примерно в 1,5 раза большую дальность действия, оказывается как нельзя кстати.

Особенности стандарта IEEE 802.3bq

До последнего времени официальная фиксация параметров кабельной техники выполнялись фактически несколько раз, причем процессы стандартизации были во многом независимы друг от друга. Такое положение определялось особенностями разработки стандартов, которые из-за разных требований к предельно допустимым значениям образовали иерархическую структуру (рис. 1).

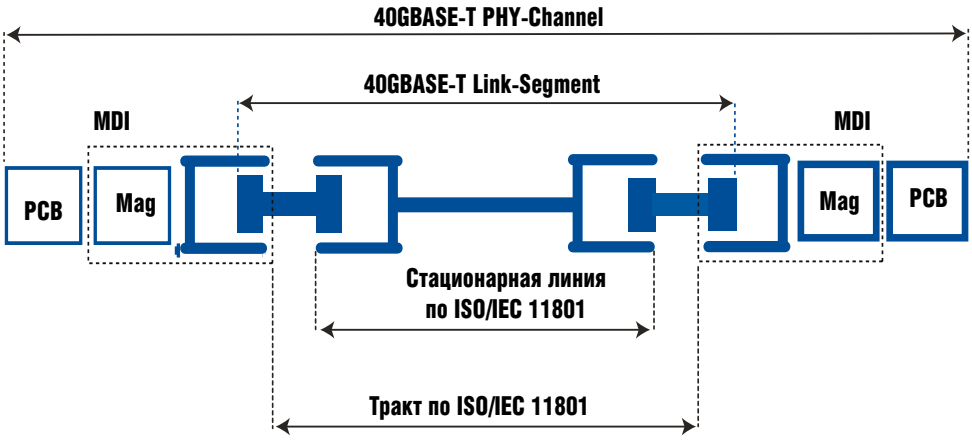


Рис. 2. Комплексные объекты IEEE 802.3bg и их взаимное соответствие

Разработчики сетевых интерфейсов ориентируются на текущий уровень техники, минимальные требования к которой фиксируются в спецификации IEEE. Уже на первом этапе работы над интерфейсом они официально выдаются в форме технического задания кабельной промышленности. Последняя на их основе формирует свои стандарты, учитывая при этом свой задел и имея некоторое время на улучшение характеристик. Кроме того, в соз-

даваемый стандарт дополнительно закладывается некоторый запас, чтобы компенсировать ухудшение характеристик линии в процессе прокладки, старения элементов и т.д.

Возможен также вариант пересертификации. Он был задействован, например, при переходе от техники 5 к 5e и был отражен в американском документе TSB-95. Промежуточный характер требований этого бюллетеня обусловлен тем, что большинство линий категории 5, которые потенциально могли быть адаптированы к работе на скорости 1 Гбит/с, создавались на уже отработанной в серийном производстве технике. Фактически они гарантированно отвечали требованиям более строгим, нежели те, что содержатся в спецификациях IEEE, созданных ранее для интерфейсов Fast Ethernet.

Вновь вводимые интерфейсы 25GBASE-T обеспечивают промежуточное значение скорости и не требуют новой элементной базы. Описывающий их стандарт IEEE 802.3bq рассматривает линию связи как единое целое исходя уже из существующего физического уровня. Допустимы только двухконнекторные структуры линий. Последнее означает возможность подключения оборудования только по схеме интерконнекта, использование консолидационной точки не предусматривается.

Параметры линии стандарта IEEE 802.3bq оптимизируются исходя из полной вложенности четырех комплексных объектов (рис. 2). Два из них являются классической стационарной линией и полным простым трактом СКС. Так называемый 40GBASE-T Link-Segment представляет собой тракт СКС, дополненный двумя вилками соединительных шнуров. Полный физический тракт 40GBASE-T PHY-Channel заканчивается на обоих концах выходом печатной платы PCB линейного модуля сетевого интерфейса. Это важно с аппаратурной точки зрения, так как позволяет унифицировать по посадочным местам и раскладке контактов электропроводный и волоконно-оптический варианты сетевого интерфейса. Вложенный характер комплексных объектов и их заранее известные характеристики не только обеспечивают бесшовный переход между аппаратурой и пассивной частью канала связи, но и позволяют улучшить качество связи за счет точного согласования их параметров.

Возможности сочетанного использования техники категории 8 и 25GBASE-T

Элементная база категории 8 может быть только экранированной. Она существует в двух вариантах, обозначаемых как 8.1 и 8.2. Решение 8.1, прототипом которого является F/UTP-техника категории 6a, имеет несколько худшие параметры по взаимным влияниям. Чтобы их компенсировать, в штатном цифровом сигнальном процессоре DSP-приемника сетевого интерфейса осуществляется сложная многоступенчатая обработка смеси сигнала с шумом. Выполнение большого объема вычислений сопровождается увеличением нагрузки на источник питания сетевой аппаратуры и, соответственно, повышенным тепловыделением, что для ЦОДа нежелательно. С этой точки зрения выгоднее применять технику категории 8.2 с индивидуальным экранированием витых пар, серийные образцы которой доступны в исполнении F/FTP или SF/FTP.

Полная протяженность кабельного тракта категории 8, согласно действующему стандарту, не зависит от исполнения кабельных изделий. Длина тракта зависит только от калибра токопроводящих жил витых пар и колеблется в пределах 28–32 м. Уменьшение частоты Найквиста линейного сигнала интерфейса 25GBASE-T до 1,04 ГГц минимизирует влияние этого фактора и дает возможность не учитывать его при планировании сети. Кроме того, более экономное использование частотного диапазона позволяет увеличить протяженность тракта до 40 м и более, а также открывает перспективы применения оборудования 25GBASE-T с кабельными трактами категории 7a. Последняя возможность не предусматривается спецификацией IEEE 802.3bq, но ее реализация не имеет серьезных ограничений, поскольку в качестве прототипа кабельной техники категории 8.2 использована элементная база категории 7a, пересертифицированная для работы в частотном диапазоне до 2 ГГц.

Внедрение 25-гигабитных медножильных сетевых интерфейсов Ethernet отвечает потребностям современного этапа развития техники локальных сетей.

Появление стандарта сетевых интерфейсов IEEE 802.3bq может способствовать расширению использования электропроводной техники в машзалах ЦОДов.

Сетевые интерфейсы IEEE 802.3bq не требуют разработки новой техники физического уровня канала связи и изначально рассчитаны на работу по кабельным трактам категории 8.

Резервы пропускной способности, которые появляются за счет более экономного использования рабочего частотного диапазона, можно направить на увеличение дальности связи. ИКС

Медицина обретает цифровой контур

Александра Крылова

«Компьютеризация» – «информатизация» – «цифровизация» – таковы основные этапы затянувшегося пути здравоохранения к насыщению современными информационными технологиями, двигаться по которому ему предстоит по крайней мере до конца 2024 г. Вопросы: «К чему идем? Куда хотим прийти?» требуют детального рассмотрения.

Основа для цифровизации

Постановление Правительства РФ от 5.05.2018 № 555 «О единой государственной информационной системе в сфере здравоохранения» подвело черту под действующей концепцией информатизации. Новый документ оставил за ЕГИСЗ только федеральный сегмент, отделив от нее информационные системы регионального уровня и уровня медицинских организаций, и сфокусировал ее на агрегации отраслевой статистики и управленческой информации.

Системы, призванные обеспечить хождение электронных рецептов и учет льготных лекарственных средств, будут внедряться на уровне регионов, т.е. в РМИС или, как их теперь называют, государственные информационные системы (ГИС) в сфере здравоохранения субъектов РФ. Персонализированные интегрированные электронные медицинские карты (ИЭМК) будут вестись и храниться в медицинских информационных системах медорганизаций (МИС МО), а в одноименной подсистеме ЕГИСЗ эти данные будут содержаться в деперсонифицированном виде.

Для обмена информацией подсистемы ИЭМК медицинской организации с внешними системами будет использоваться Регистр электронных медицинских документов (РЭМД) – подсистема, входящая в состав ЕГИСЗ.

Изменения в роли ЕГИСЗ были подхвачены и развиты при подготовке паспорта Национального проекта «Здравоохранение», в составе которого есть проект федерального значения «Создание единого цифрового контура в здравоохранении на основе ЕГИСЗ». За его реализацию будет отвечать заместитель министра здравоохранения Российской Федерации Наталья Хорова. Заявленная цель проекта – создание механизмов цифрового взаимодействия медицинских организаций на основе ЕГИСЗ. А основные направления, в которых он будет развиваться, – внедрение и развитие медицинских информационных систем во всех медицинских организациях и электронный медицинский документооборот между медорганизациями и органами управления здравоохранением.

Таким образом, ЕГИСЗ в новом своем качестве становится мостом между программой информатизации российского здравоохранения и федеральным проектом, направленным на его цифровизацию, обеспечивая эволюционное развитие процесса, а значит, сбережение уже сделанных в него на разных уровнях инвестиций.

Вместе с тем, признают эксперты, термины «электронное здравоохранение» и «цифровое здравоохранение» пока не устоялись и границы между ними размыты. Интересную точку зрения на этот счет высказал Георгий Лебедев, директор Института цифровой медицины и завкафедрой информационных и интернет-технологий Первого МГМУ им. И.М. Сеченова. Он считает, что Федеральным законом от 29.07.2017 № 242-ФЗ были созданы правовые основы для электронного здравоохранения: регламентировано применение ЕГИСЗ, легализованы оказание медицинской помощи с использованием телемедицинских технологий и электронный документооборот в медицинских организациях. А цифровая медицина – это надстройка над системами электронного здравоохранения в виде математических методов и алгоритмов, которые применяются при обработке больших данных для поддержки принятия решений врача в экспертных системах. И разработка ее правовых основ регулятору и профессиональному сообществу еще предстоит.

80% ГОСЗАКАЗА НА ИНФОРМАТИЗАЦИЮ ЗДРАВООХРАНЕНИЯ ТРАТЯТ **15** ВЕДУЩИХ РЕГИОНОВ вместе с г. Москва

Источник: НИУ ВШЭ

Телемедицина де-юре и де-факто

Как показали первые девять месяцев, миновавшие после вступления закона № 242-ФЗ в силу, реализация его норм внутри медицинских организаций – дело нелегкое. Существуют нерешенные вопросы регуляторного характера. Есть и определенные технические сложности: для консультаций в формате «врач – пациент» барьером яв-

«Цифровой контур» здравоохранения

Из доклада Е. Бойко «О создании единого цифрового контура в здравоохранении Российской Федерации» 11 октября 2018 г. на международном конгрессе «Информационные технологии в медицине»

Михаил Плисс

Требуется провести аудиты технических стандартов, определить уровень и квалификацию специалистов, которые могут проводить телемедицинские консультации, так организовать работу, чтобы в их распорядке дня были оплачиваемые по тарифам ОМС слоты времени на дистанционную помощь коллегам и пациентам.

ляется идентификация участников телемедицинского сеанса в Единой системе аутентификации и идентификации.

«Наша система оказания медицинской помощи такова, что все деньги, которые выделяются ОМС на телемедицину, получает та медорганизация, которая ведет пациента», – комментирует ситуацию Михаил Плисс, заместитель директора департамента по экспертно-аналитической работе НИУ ВШЭ. А оплата услуг опытного врача, выступающего в роли консультанта, в телемедицинском тарифе в некоторых регионах вообще не оговорена.

Для того чтобы телемедицинские технологии начали активно внедряться в практику оказания услуг медицинской помощи, действующей нормативной правовой базы мало: нужна большая организационная работа по оснащению кабинетов для дистанционных консультаций, пересмотру действующих бизнес-процессов и регламентов.

Игорь Шадеркин, завотделом региональной урологии НИИ урологии и интервенционной радиологии им. Н.А. Лопаткина, в котором консультировать пациентов дистанционно по различным каналам связи начали еще до принятия 242-ФЗ, считает ожидаемые выгоды от применения телемедицинских технологий несколько преувеличенными. По его мнению, вряд ли они сделают услуги высококвалифицированных специалистов доступней. «У хорошего врача всегда есть пациенты, а вот времени свободного очень мало, – говорит он. – Конечно, на платную консультацию время, может быть, найдется, но все равно мы упремся в ограниченное количество высококвалифицированных специалистов».

К тому же применение дистанционных медицинских технологий, по его мнению, не облегчает работу врачей. Напротив, количество обращений, к примеру, хронических больных увеличивается.

Выход из сложившейся ситуации эксперт видит в «вооружении» пациентов медицинскими приборами для дистанционного мониторинга состояния здоровья и простыми средствами аналитики – инструментами, в том числе автоматическими, которые позволят людям корректировать свой образ жизни в соответствии с их рекомендациями.

Эволюционное движение

В Федеральном законе № 242-ФЗ есть нормы, обязывающие Минздрав России регламентировать использование в медицинских организациях документов в электронной форме. В начале 2018 г. ведомством был принят приказ №2н, вносящий изменения в приказ этого же ведомства от 15.12.2014 № 834 «Об утверждении унифицированных форм медицинской документации, используемых в медицинских организациях, оказывающих медицинскую помощь в амбулаторных условиях, и порядков по их заполнению». Новым приказом, в частности, разрешается ведение медицинских документов как в бумажном, так и в электронном виде, но «в порядке, установленном Минздравом России». Между тем как раз единого для амбулаторных и стационарных учреждений порядка ведения электронных документов нет. А по мнению Бориса Зингермана, члена Экспертного совета по ИКТ Минздрава РФ, единый регламент, объясняющий, как вести медицинские документы в электронной форме, необходим.

Нельзя сказать, что движения в этом направлении нет. По словам Татьяны Зарубиной, глав-

МНЕНИЕ ЭКСПЕРТА

Экспертным системам нужна верификация

Георгий Лебедев, директор Института цифровой медицины, завкафедрой информационных и интернет-технологий, Первый МГМУ им. И.М. Сеченова

Следующим шагом за созданием в России правовых основ электронного здравоохранения, должно стать построение нормативного базиса цифровой медицины. Начинать разработку такого базиса нужно с классификации решений, которые могут применяться в цифровой медицине (речь идет о математических методах, включая методы искусственного интеллекта). На втором этапе должна быть построена система стандартов и нормативных правовых документов, определяющая требования к используемым программным средствам, методики подтверждения соответствия алгоритмов и математических методов тем медицинским задачам, для решения которых они предназначены. В частности, мы должны понимать, какой объем медицинских данных должен быть обработан экспертной системой, какая выборка данных позволяет получить наиболее правильное решение той или иной медицинской проблемы.

Но самое главное – четко указать в нормативных документах, что любая система для

ного внештатного специалиста по внедрению ИС в здравоохранении Минздрава России, заместителя директора ЦНИИОИЗ МЗ РФ и завкафедрой РНИМУ им. Н.И. Пирогова, уже определены структура документов, направляемых в подсистему федеральной ИЭМК ЕГИСЗ, их кодирование и формат передачи информации.

К тому же тот факт, что электронный документооборот между всеми медицинскими организациями, органами здравоохранения выбран одним из двух направлений федерального проекта «Создание единого цифрового контура в здравоохранении на основе ЕГИСЗ», свидетельствует о понимании регулятором важности этого вопроса. Правда, становится ясно, что его решение планово растянется до 2024 г., срока, к которому должен быть реализован Национальный проект «Здравоохранение».

Новые зоны для законотворчества

Эксперты в области информатизации здравоохранения признают, что после создания основ для электронного здравоохранения нужно создавать правовую базу для цифровой медицины, включающей в себя экспертные системы и системы поддержки принятия врачебных решений, а также применение технологий и устройств медицинского интернета вещей. И всевозможные «умные» приборы, и сложные интеллектуальные продукты – математические методы и алгоритмы, которые используются в экспертных системах, требуют, по их убеждению, проведения клинических испытаний, верификации и сертификации.

Эта позиция вступает в противоречие с точкой зрения представителей институтов развития, убежденных в том, что для инновационных разработок медицинских стартапов подобные процедуры должны быть упрощены. Позиция последних закреплена в нормативной «дорожной карте» – плане мероприятий по совершенствованию законодательства и устранению административных барьеров, разработанном в поддержку развития Национальной технологической инициативы по направлению «Хелснет».

В этом документе, утвержденном по стечению обстоятельств также 5 мая 2018 г., предусмотрена разработка 25 новых нормативных актов, регулирующих спорные вопросы использования цифровых технологий в медицине, в период с 2018 по 2035 гг.

Как организовать проверку адекватности технологических разработок – аппаратных и программных средств, помогающих людям следить за состоянием своего здоровья, чтобы лучшие из них быстро находили дорогу к пациентам? Вопрос, ответить на который еще предстоит.

> Если раньше пациент приходил на прием один раз в два месяца, то благодаря телемедицинским технологиям он получает возможность «стучаться» ко мне каждый день.


Игорь Шадеркин

МНЕНИЕ ЭКСПЕРТА

сферы здравоохранения, применяющая цифровые методы обработки больших медицинских данных, включая системы искусственного интеллекта и системы интеллектуальной поддержки принятия врачебных решений (СППВР), должна работать исключительно внутри медицинских организаций. Это необходимо для того, чтобы не допустить применения подобных интеллектуальных систем компаниями, не имеющими лицензий на оказание медицинской помощи.

Ответственность за соблюдение порядка применения СППВР и экспертных систем предлагаем возложить на главных врачей, обязав их следить за тем, чтобы каждый доктор, прибегающий к автоматически сгенерированным рекомендациям, понимал, как они могут быть использованы в лечении того или иного пациента.

В условиях, когда тема искусственного интеллекта набирает популярность среди разработчиков и многие занимаются глубоким обучением нейронных сетей, необходима проверка и оценка адекватности математического метода. Для этого в новый нормативный правовой документ необходимо включить требование об обязательных клинических испытаниях всех СППВР с последующей регистрацией в Росздравнадзоре как технологии или как медицинского изделия. А это значит, что предстоит строить базис для клинических испытаний, выбирать средства верификации этих систем, а также контроля непротиворечивости предлагаемых ими решений.

Борис Зингерман

В медицинском документообороте сегодня существует целый клубок проблем, которые нужно решить, и, к сожалению, он такой большой, что медорганизациям проще вести документацию и в бумажном, и в электронном виде.

Словом, для того чтобы включить в единый цифровой контур все необходимые для качественной работы врачей и полезные для повышения продолжительности жизни россиян программные и аппаратные средства, регулятору, профессионалам в области медицины и информатизации здравоохранения, экспертам институтов стратегического управления и институтов развития предстоит еще большая работа.

Если МИС МО не облегчает работу врача – значит, что-то не так с системой

О значении перемен в электронном здравоохранении, вызванных новым положением о ЕГИСЗ, – Татьяна Зарубина, главный внештатный специалист по ИС в здравоохранении Минздрава России,заместитель директора ЦНИИОИЗ МЗ РФ и завкафедрой РНИМУ им. Н.И. Пирогова.

– В Положении «О единой государственной системе в сфере здравоохранения», утвержденном Постановлением Правительства РФ № 555 от 05.05.2018, двухуровневая архитектура подверглась переосмыслению и пересмотру. Однако ЕГИСЗ (ФГИС) не только не утратила своего значения, а наоборот. На ее основе в отрасли будет создаваться единый цифровой контур в рамках Национального проекта «Здравоохранение». Уже разработан паспорт федерального проекта. Идет работа над региональными проектами «Создание единого цифрового контура в здравоохранении на основе ЕГИСЗ». Каждый субъект готовит паспорт с учетом уровня информатизации своих медицинских организаций, региона в целом.

Региональные медицинские информационные системы, РМИС, превратились в государственные информационные системы в сфере здравоохранения субъектов РФ, и это изменение, считаю, должно повысить уровень ответственности регионов. При этом проблема совместимости информации никуда не делась: ЕГИСЗ – система федерального уровня – должна получать информацию из систем субъектов РФ. Для обеспечения совместимости разработаны протоколы обмена, определены структура электронных медицинских документов, кодирование и формат передачи информации в подсистему интегрированной электронной медицинской карты (ИЭМК). Начал функционировать федеральный реестр электронных медицинских документов.

– Когда заходит речь об интеграции МИС разных уровней, возникает ассоциация с системой межведомственного электронного документооборота, предназначенного для обмена электронными документами между ИС органов власти. Будет ли создаваться что-то подобное в здравоохранении?

– Шаги в сторону межведомственного взаимодействия уже делаются: структурированные электронные медицинские документы для этого разработаны и используются. СЭМД «Медицинская справка о допуске к управлению транспортным средством», «Медицинское свидетельство о рождении», «Медицинское свидетельство о смерти» модернизированы до 3-го уровня архитектуры клинических документов, т.е. в них максимально используется кодирование информации.

Определенные перспективы связаны с Реестром электронных медицинских документов (РЭМД), подсистемой ЕГИСЗ, которая должна предоставлять пациенту его медицинские документы, а также обеспечивать, с его ведома, взаимодействие с внешними системами и передачу документов между МО, МИС МО и ГИС в сфере здравоохранения субъектов РФ.

Кроме того, вместе с Федеральным фондом ОМС, мы приступаем к гармонизации нормативно-справочной информации для того, чтобы справочники, которыми пользуются сотрудники федерального и территориальных фондов, играющих важную роль в жизни каждой медорганизации, и справочники, к которым обращаются врачи, были едиными. Движение к унификации началось: проведен анализ справочников ФОМС и Минздрава России.

– Согласно положению о ЕГИСЗ, информация о пациентах должна храниться в федеральной подсистеме ИЭМК в обезличенном виде. Значит, врачи лишаются возможности

быстро получать из нее медицинские данные пациентов в экстренных ситуациях?

– При использовании единого хранилища возрастают риски взлома и утечки информации. Можно, конечно, сделать федеральное хранилище ИЭМК распределенным и тем минимизировать риски, но это намного дороже. Задача преемственности оказания медицинской помощи обеспечивается РЭМД и ГИС в сфере здравоохранения субъектов РФ, т.е. разными сегментами цифрового контура. В нашей системе здравоохранения, отличающейся от систем ряда западных стран высоким уровнем централизации и вертикализации функций и информации, это возможно.

При этом задача оценки здоровья популяции остается важнейшей задачей федеральной ИЭМК.

– Одним из ожидаемых результатов создания единого цифрового контура российского здравоохранения на основе ЕГИСЗ должно стать внедрения систем электронных рецептов на уровне регионов. Что предстоит сделать для его достижения?

– В реализации подсистемы электронного рецепта участвуют врач, пациент и аптечная организация, в которую пациент обращается за препаратом. Необходимо иметь и обратную связь, чтобы информация о факте покупки лекарства попадала в подсистему ГИС субъекта РФ. Здесь есть нюанс: в некоторых регионах большинство аптек частные и потому не обязано пока такую прозрачность обеспечивать. Но двигаться к этому нужно, потому что все, что касается сферы здравоохранения, должно быть прозрачно. Это должно быть требованием к ГИС субъектов в части реализации электронных рецептов.

В большинстве регионов функционируют подсистемы, обеспечивающие передачу льготных рецептов. В части льготного лекарственного обеспечения взаимодействие по реализации электронных рецептов записано в контрактах с аптечными организациями.

Есть регионы, где электронный рецепт уже полноценно работает. Но есть и такие, где подключение всех медорганизаций еще предстоит реализовать.

– Насколько внедрение МИС в медицинских организациях (к 2024 г. оно должно стать повсеместным) облегчает работу врача?

– Сначала не облегчает, потому что врач пока еще часто не подготовлен. Правда, я видела в регионах молодых докторов, которые обращаются с системой как продвинутые пользователи. Однако для врачей старших возрастных групп обучение может быть проблемой. Но она разрешима. Просто потребуется больше терпения и времени.

Организаторами здравоохранения субъектов РФ проработаны и запланированы системные мероприятия по обучению и повышению квалификации врачей в части применения информационных систем.

Обычно сразу после внедрения МИС МО наблюдается даже замедление работы медицинского персонала, но в течение года ведение электронных медицинских карт становится для медиков рутинной задачей, и они уже не представляют, как можно работать по-другому. Если этого не происходит, значит, что-то не так с системой.

Уже не сомневаюсь, что к концу 2021 г. МИС МО будут распространены повсеместно, в соответствии с паспортом федерального проекта.

– Можно ли сказать, что уже сегодня МИС МО – источник больших медицинских данных, анализ которых позволит врачам и ученым найти решение многих проблем?

– До Big Data мы еще не дожили. Пока речь идет об обработке объединенных данных, накопленных в нескольких медицинских учреждениях, особенно если в них используется одна и та же МИС МО. Мы имеем на это право, поскольку в таком случае применяются одинаковые справочники и часто – в однопрофильных учреждениях – сопоставимые схемы ведения пациентов. Серьезные надежды в плане источника Big Data можно возлагать на федеральную ИЭМК. Конечно, если в нее из МИС МО в массовом порядке будут передаваться структурированные электронные документы с высоким уровнем кодирования медицинской информации.

МИС МО нацелена на автоматизацию лечебно-диагностического процесса, но она, конечно, является источником и инструментом для создания электронных медицинских документов, которые станут основой для реализации подхода больших данных.

– Есть ли подходы к автоматизации клинических рекомендаций, за внедрение которых в процесс оказания медицинской помощи ратует Минздрав России?

– Тут надо провести четкую грань между справочными информационными системами, объясняющими, как использовать клинические рекомендации, системами, снабженными модулями, которые обеспечивают сравнение того, что было сделано пациенту, с клиническими рекомендациями по нозологии и выводят соответствующую форму представления, и подсистемами МИС, обеспечивающими встраивание рекомендаций в лечебно-диагностический процесс. Это задачи разного уровня. Первый вид систем уже распространен, и это правильно, потому что справочная информация врачам нужна и полезна. Второй вариант тоже встречается часто. Что касается третьего, то это сложная задача, хотя бы потому, что для ее реализации нужно определять, что и куда встраивать, и буквально «перелопачивать» всю МИС медицинской организации.

Скажу больше, для превращения клинических рекомендаций в алгоритмы, встроенные в МИС МО, нужно проделать большую предметную работу. По-хорошему, она должна осуществляться путем построения онтологий предметной области с помощью привлечения экспертов высокого класса и фактически превращения того, что написано в клинических рекомендациях, в экспертные системы, встроенные в МИС МО. Но за этим будущее. И клинические рекомендации – значимый шаг в этом направлении.

От электронных документов – к цифровым сервисам

Борис Зингерман, руководитель направления цифровой медицины, INVITRO, член Экспертного совета по ИКТ Минздрава России

Что мешает медицинским организациям и органам управления здравоохранением полностью перейти на электронный документооборот и что приобретут врачи и пациенты, когда такой переход произойдет?

Барьеры на пути ЭДО

Ключевой вопрос, который беспокоит медиков, – доверие к электронным документам со стороны проверяющих органов, коих в здравоохранении множество. Пока медицинским организациям приходится доказывать, что они имеют право при проверках предоставлять документы в электронном виде.

Другая, не менее существенная для медицинских организаций проблема – высокая стоимость перехода к электронному документообороту (ЭДО). Ключи электронной цифровой подписи (ЭЦП) должны быть у многих сотрудников медучреждения. Срок действия ЭЦП – год, а ее среднерыночная цена – 3 тыс. рублей. Если учесть, что каждому врачу может понадобиться не одна электронная подпись, а три (для электронных больничных, для электронных рецептов и для других медицинских документов), то становится понятно, что для большинства медицинских организаций это дорогое удовольствие.

В 2006 г. Гематологическим научным центром РАМН был разработан ГОСТ 52636-2006 «Электронная история болезни. Общие положения», в котором предлагается обеспечить подписной процесс и систему доверия к документам внутри медицинской организации более дешевым способом. Для этого медорганизация должна принять внутренний регламент функционирования ЭДО. Конечно, при необходимости передачи электронного документа за пределы медорганизации заверять его электронной подписью придется. Но поскольку все исходящие документы подписываются представителями руководящего звена, то средств на приобретение ЭЦП медицинской организации понадобится существенно меньше. Если же документ подписан лечащим врачом, то его подпись своей ЭЦП удостоверяет заведующий отделением или главный врач. Иногда за копией документа, подписанного в МИС МО, обращается пациент. В этом случае сотрудник, имеющий право ее выдать, удостоверяет своей «бумажной» или электронной подписью, что этот документ является бумажной копией электронного документа, хранящегося в системе.

Поскольку одномоментный переход к электронному медицинскому документообороту невозможен, медорганизациям предстоит довольно длительный период смешанного документооборота, при котором электронные документы сосуществуют с бумажными. Для этого требуется отдельный регламент. В октябре 2016 г. на заседании Экспертного совета по ИКТ Минздрава мною был представлен проект положения о смешанном документообороте, в котором, в частности, содержался запрет на внесение рукописных дополнений в бумажные копии электронных документов, а также был определен приоритет электронной версии для таких документов. Этот проект был одобрен экспертным советом, но дальнейших действий не последовало.

Кроме того, серьезный барьер для автоматизации документооборота медорганизаций – действующие ныне формы медицинских документов, частью архаичные и не подлежащие переводу в электронный вид. Например, не всегда понятно, как в таком документе после оцифровки различаются его лицевая и оборотная стороны или как организовать его последовательное заполнение несколькими людьми.

Ситуацию мог бы исправить нормативный документ Минздрава России, который установил бы, что формы медицинских документов могут быть пересмотрены при сохранении содержания, т.е. разрешил бы так перестроить существующие в них поля, чтобы их можно было перевести в электронный вид. Также важно, чтобы все новые приказы или письма отраслевого ведомства, в которых фигурируют какие-либо формы электронных документов, четко регламентировали их бумажный и электронный вид. Пока этого, к сожалению, не происходит.

Надо понимать, что все перечисленные выше барьеры не просто сдерживают переход медицинских организаций на ЭДО, но и вынуждают вести его и в бумажном, и в электронном виде. Главным по-прежнему остается бумажный доку-

ментооборот, но поскольку какие-то данные все равно нужно вносить в МИС, это порождает двойную работу и естественное недовольство врачей.

Эффект отмены

Между тем от полного перехода медицинских организаций на электронный документооборот выиграют и врачи, которым больше не придется дублировать электронные записи на бумаге и тем самым выполнять двойную работу, и пациенты. О выигрыше пациентов хочется рассказать немного подробнее.

Начну с того, что после внедрения в поликлиниках и стационарах электронного документооборота они, наконец, смогут воспользоваться доступом к своей медицинской документации, т.е. будут в курсе всех проблем со своим здоровьем и, возможно, начнут о нем больше заботиться.

Кроме того, чтобы помочь пациенту, у которого после приема врача, как правило, остается много вопросов, доктор мог бы в полуавтоматическом режиме прикреплять к электронному документу с заключением несколько информационных ссылок на проверенный и признанный в медорганизации источник. Перейдя по этим ссылкам из своего медицинского документа, пациент получит достоверное описание своей проблемы и назначенного лечения. К сожалению, врач почти никогда не успевает «поговорить» с пациентом, а предложенная система позволит пациентам дома спокойно прочесть то, что врач не успел сказать.

К такому заключению впоследствии можно будет добавить и другие персонализированные сервисы. Так, если врач назначил какое-либо лекарство, пациент может установить мобильное приложение, которое напомнит о необходимости его приема, может приобрести гаджет, позволяющий проводить измерения, сохранять их в базе данных и, возможно, передавать их своему врачу.

Тут мы переходим к телемедицине в широком смысле слова, подразумевающем дистанционное взаимодействие пациента с лечащим врачом и с системой здравоохранения в целом. К примеру, при выписке из стационара человек останется под наблюдением того же врача, который вел его в клинике и продолжит наблюдать его, только теперь дистанционно, в период реабилитации. При этом лечащий врач сможет дистанционно отвечать на возникающие у пациента вопросы.

Конечно, такой подход увеличивает нагрузку на врача, но части пациентов подобные сервисы могут предлагаться на платной основе. Скажем, определенный объем услуг – очный прием доктора – покрывается из фонда ОМС. А с тех, кто хочет получить необходимую информацию без дополнительного приема, можно брать плату за превышающий этот объем сервис.

Иными словами, будущее здравоохранения неразрывно связано с цифровыми сервисами, от записи пациента к врачу через интернет и дистанционного наблюдения лечащим врачом к электронным рецептам, которые существенно помогли бы хроническим больным, и к доставке по этим рецептам лекарств.

Частная медицина в ожидании консолидации

Догнать государственные медучреждения по уровню информатизации частные российские клиники смогут тогда, когда медицинский рынок в стране пройдет процесс консолидации.

Михаил Плисс, заместитель директора департамента по экспертно-аналитической работе, НИУ ВШЭ

В нашей стране на рынке медицинских услуг доля частной медицины (в денежном выражении) составляет около 4%. Самая крупная российская сеть коммерческих клиник – «Мать и дитя» – занимает менее 1%. На долю государства приходится примерно 96% рынка стационарной и примерно 74% поликлинической медицинской помощи.

В России коммерческие медицинские организации по уровню информатизации уступают государственным. Только небольшое число клиник считают ИТ своим конкурентным преимуществом. Остальные относятся к информатизации как к налогу на бизнес, поскольку явной прибыли медицинские информационные системы им пока не приносят. Так что у меня есть сомнения в том, что российские частные клиники смогут выполнить требование об обязательном предоставлении информации о своей деятельности в ЕГИСЗ, которое вступает в силу с 1 января 2019 г., особенно если за неисполнение этого требования их никто не накажет.

В США для того, чтобы поддержать клиники при переходе на информационные системы, была разработана двухэтапная программа мотивации Meaningful Use. Первый этап предполагал вознаграждение в виде освобождения от налогов компаний – лидеров этого движения, а второй – штрафы для тех клиник, которые задержались с внедрением ИТ-систем. То есть даже в Америке были госпитали и больницы, которые не спешили вкладываться в МИС.

И это понятно, поскольку в мировой практике здравоохранение – одна из самых дорогих областей информатизации: для госпиталя на 500 коек средняя стоимость современной

За результатами приема – в личный кабинет

Клиенты ГК «Медси» могут воспользоваться мобильным приложением SmartMed для получения с помощью своих смартфонов дистанционных консультаций по видеосвязи или в чате как с врачами-терапевтами и педиатрами, так и с узкими специалистами: аллергологами, гастроэнтерологами, кардиологами и т.п. Все заключения, которые выдаются после телемедицинских консультаций, заверяются электронной цифровой подписью врача.

В приложении, работающем на iOS- и Android-устройствах, пациентам из любой точки мира доступны запись на очный прием в клиники и центры компетенции ГК «Медси», заказ плановых и срочных онлайн-консультаций, данные из их медицинской карты, а также обмен медицинскими документами, например результатами исследований, с врачами.

Приложение SmartMed соответствует требованиям Минздрава России к оказанию услуг с применением телемедицинских технологий, так что пациенты «Медси» могут быть спокойны за сохранность и защищенность своих персональных медицинских данных. За техническое обеспечение услуги отвечает партнер сети частных клиник – оператор МТС, организовавший хранение медицинской информации в защищенном сегменте своего облака #CloudMTC, где развернут комплекс специализированных решений безопасности, аттестованных по требованиям ФСТЭК, в том числе системы сертифицированной криптографической защиты каналов связи, антивирусной защиты, противодействия угрозам несанкционированного доступа и анализа уязвимостей.

МИС, автоматизирующей значимую часть бизнес-процессов клиники, начинается с $25 млн.

Высокая цена обусловлена несколькими факторами. Во-первых, повышенной надежностью таких систем, поскольку цена ошибки – жизнь человека. Во-вторых, высокой наукоемкостью, так как автоматизация медицинских процессов связана с алгоритмизацией не только законодательства, но и медицинской практики, и научных публикаций. В-третьих, большими вложениями в оптимизацию работы медицинских работников.

Последнее требует пояснения. Почти во всем мире, за исключением России и стран СНГ, врач – одна из самых высокооплачиваемых профессий. Все минуты и секунды, потраченные им впустую, складываются в огромные убытки. Поэтому сейчас разработчики уделяют огромное внимание удобному интерфейсу медицинских систем, стремясь уменьшить до минимума время выполнения любых операций с компьютером во время приема пациента.

Врач в ходе приема использует компьютер не так, как это делают бухгалтеры, программисты или логистики. Врач общается с пациентом, и на несколько секунд должен отвлечься от него к компьютеру, внести всю необходимую информацию и вернуться к разговору с пациентом. Для того чтобы это было возможно, логика и удобство работы программы, «юзабилити», должны находиться на высочайшем уровне. К сожалению, дизайн и оптимизация – не самые сильные стороны отечественной школы разработки.

Неудивительно, что системы, которые успешно оптимизируют дорогое рабочее время дорогих специалистов, стоят миллионы долларов и что они окупаются там, где врачи дорогие.

Также неудивительно, что даже самые крупные российские частные клиники не могут себе позволить информационную систему такого уровня. Согласно известной модели Gartner, показывающей, какую часть оборота разные отрасли тратят на ИТ, медицинские организации выделяют на эти цели сейчас 2%, а в будущем эта цифра вырастет до 3–4%. Для того чтобы внедрить МИС стоимостью $25 млн, оборот коммерческой клиники должен составлять $500 млн. Понятно, что таких клиник сегодня в России нет.

Надо признать, что развитие частных медицинских организаций в России сдерживается экономическим кризисом. У частника в основном три канала получения прибыли: наличные платежи, выплаты от страховых компаний по программам государственного обязательного медицинского страхования и частного добровольного медицинского страхования.

Под воздействием кризиса объем рынка добровольного медицинского страхования, а именно он является основным источником дохода коммерческой медицины, уменьшился вдвое. Объясняется это просто: в отличие от западного рынка таких услуг, наш рынок ДМС ориентирован исключительно на корпоративный сегмент. А компании в условиях экономической и финансовой нестабильности стали сокращать и страховые покрытия, и количество застрахованных. В результате мы наблюдаем сегодня двукратное уменьшение объема рынка и такой же рост цен на услуги частных медицинских организаций.

Наличных денег у беднеющего населения все меньше и меньше, а тарифы ОМС не всегда могут покрыть затраты.

Вроде бы кризис должен поднимать уровень управленческой компетентности, заставлять повышать эффективность. Но по уровню управ-

Доля оборота, затрачиваемая на ИТ предприятиями различных отраслей

Источник: Gartner

ленческой компетенции и экономической эффективности российские частные клиники тоже сильно отстают и от европейских, и от израильских, и от американских и японских. За рубежом происходит не просто оптимизация процессов на уровне клиник, происходит консолидация клиник и оптимизация работы огромных медицинских холдингов.

В результате многочисленных сделок по слиянию и поглощению в этой сфере в мире образовались мощные сети из 400–500 клиник, возглавляемые профессиональными медицинскими управляющими компаниями и живущие по модели гостиничного бизнеса. У каждой из таких сетей клиник большие возможности экономии за счет масштаба. К примеру, лекарственные препараты и медицинское оборудование они закупают с огромными скидками. А вся их экспертиза по процессам оказания медицинской помощи «зашита» в ИТ-системы, которые развиваются ими на протяжении 20–30 лет.

Возможно, крупные сети частных клиник в России появятся позже, когда рынок нашей коммерческой медицины консолидируется. Пока же я вижу, что повышению ее эффективности могут способствовать новые игроки – поставщики решений для медицинских организаций по расшифровке кардиограмм, описанию рентгеновских изображений, проведению лабораторных анализов. По сути, нас ждет формирование рынка медицинского аутсорсинга.

Перевод частными клиниками не связанных напрямую с лечебным процессом функций на сервисную модель позволит им экономить средства на зарплате штатным специалистам, сократить время предоставления результатов исследований пациентам, а значит, повысить их лояльность. На мой взгляд, потенциал рынка подобных медицинских сервисов огромный. Места на нем хватит для многих новых игроков, и тут нас ждет много историй успеха.

Интернет медицинских вещей в профилактических целях

Рынок интернета медицинских вещей в России только формируется, но очень быстрыми темпами. Как могут вписаться в единый цифровой контур здравоохранения «домашние» измерительные приборы?

Игорь Шадеркин, заведующий отделом развития региональной урологии НИИ урологии и интервенционной радиологии им. Н.А. Лопаткина – филиала НМИЦр МЗ РФ

Всю область здравоохранения можно разделить на два больших сектора: область медицины, имеющей дело с заболевшими людьми, с симптомами, диагнозами и инструментами лечения, и область здоровья. В первом секторе уже существует множество различных медицинских решений – диагностических, лечебных, фармакологических. Для людей, которые находятся во втором секторе, пока здоровы и стремятся оставаться таковыми как можно дольше, инструментов, позволяющих достичь цели, немного.

50 к 10

Между тем в основе поддержания здоровья лежит профилактика. Всемирная организация здравоохранения считает, что профилактические меры гарантируют этому процессу половину успеха.

В сфере медицинского интернета вещей сегодня наблюдаются два основных тренда. Первый – консьюмеризация профессиональных медицинских приборов: они становятся компактными, мобильными, портабельными (т.е. с помощью специального мобильного приложения измерения можно передавать на хранение в облако) и доступными. Пациенты без медицинского образования могут в домашних условиях использовать, скажем, анализатор мочи или даже аппарат для проведения УЗИ, чей функционал полностью соответствует лучшим приборам экспертного класса пяти-семилетней давности.

Второй тренд заключается в том, что к медицинскому интернету вещей начинают подключаться обычные пользовательские устройства: тонометры, весы, кружки. Скажу больше, вместе с ними в комплексе начинают работать подсистемы «умного» дома, отвечающие за климат в помещении (температуру, влажность, давление, чистоту воздуха и воды).

Оба тренда можно рассматривать как драйверы роста рынка интернета медицинских вещей, в том числе в России. Для полноты картины к этим вещам можно добавить огромное количество имеющих отношение к здоровью человека аппаратных и программных средств, к примеру, фитнес-трекеров и мобильных приложений, которые уже получили достаточно широкое распространение.

Самый высокий потенциал у устройств медицинского интернета вещей в профилактике. Правда, поскольку в секторе здоровья врача рядом с пациентом нет, последнему волей-неволей приходится самому следить за показаниями приборов, а в случае их отклонения от нормы – искать информацию о возможных причинах. Надо признать, что врачи сегодня в большинстве своем не готовы

«Умное» приложение для мобильных пациентов

Сеть клиник «К+31» в марте 2018 г. предложила своим пациентам сервис личного кабинета, пользоваться которым они могут как на мобильных устройствах на платформах iOS и Android, так и через веб-браузер. Поставщиком технического решения по модели white label выступила компания ONDOC.

В личном кабинете пациенты пользуются расширенной цифровой медкартой. В автоматическом режиме из медицинской информационной системы, установленной в каждой из трех клиник сети, по защищенному каналу в обезличенном виде в сервис поступают результаты консультаций и анализов.

В обеих версиях личного кабинета: и в мобильном приложении, и в веб-версии – есть раздел для мониторинга показателей здоровья – их можно вносить вручную или передавать с фитнес-браслетов и «умных» гаджетов. Здесь же можно вести курсы приема лекарств, отмечать прогресс в самочувствии и реакцию на медикаменты.

При этом сервис личного кабинета доступен только пациенту (решение соответствует требованиям ФСТЭК и закона о «О персональных данных»). Пациент сам настраивает доступ к информации о своем здоровье: может открыть любой из его разделов – медкарту, список визитов, мониторинг показателей – своему врачу или участнику семейного профиля (члену своей семьи).

В ближайшее время к сервису личного кабинета сети частных клиник «К+31» добавятся телемедицинские консультации.

интерпретировать показания таких медицинских устройств, поскольку не обладают необходимыми для этого компетенциями и привыкли мыслить категориями болезни, а не здоровья.

Впрочем, в Минздраве России и в российском здравоохранении в целом уже сложилось понимание важности профилактики, так что со временем ситуация изменится. Недаром в рамках Национального проекта «Здравоохранение» поставлена цель к 2024 г. охватить 90% населения ежегодными профилактическими осмотрами. В нацпроект также включены мероприятия по профилактике сердечно-сосудистых заболеваний и их осложнений у пациентов из группы высокого риска. Интерес регулятора к профилактике оправдан. Ведь, как показывает опыт США, увеличение расходов на борьбу с заболеваемостью исчерпало свой потенциал: в структуре факторов, влияющих на продолжительность и качество жизни человека, доля здравоохранения ограничена 10%. Выходя же на поле профилактических мер, мы воздействуем на его образ жизни, определяющий 50% здоровья.

От чего зависит здоровье человека

Медицинские гаджеты должны быть доступными и эффективными

Однако применение пациентами устройств медицинского интернета вещей для контроля состояния здоровья и коррекции поведения сдерживается недостаточным удобством таких приборов, подчас их высокой ценой и отсутствием привычки к здоровому образу жизни. Кроме того, не все эти устройства имеют доказанную эффективность: прошли клинические испытания, лицензирование и получили допуск к использованию.

Когда задают вопрос, можно ли рекомендовать применять для наблюдения за состоянием здоровья медицинские приборы с недоказанной эффективностью, во мне борются врач и инноватор. Первый хочет быть уверен, что их применение разрешено, а второй заинтересован в том, чтобы приборы медицинского интернета вещей как можно быстрее появлялись на рынке и становились доступными для врачей и пациентов.

Я считаю, что устройства, предназначенные для «домашнего» наблюдения, нужно выносить в отдельный класс с другой системой сертификации, добровольной и упрощенной. Эксперты по каждому клиническому направлению должны определить необходимый набор тестов, которые будут проходить такие медицинские приборы, чтобы доказать свою пригодность и эффективность. При этом нужно учитывать, что границы между медицинскими приборами, которые использует для мониторинга отдельных параметров состояния здоровья пациента врач, и пользовательскими устройствами для профилактики все больше стираются, а в недалеком будущем, скорее всего, появятся решения, сочетающие и те и другие возможности.

В мире ежедневно создаются новые устройства медицинского интернета вещей для самого разного использования. В России их доступность не очень высока. Большое количество зарубежных решений требуют регистрации, а она у нас небыстрая, и потому устройств, ее успешно прошедших, немного. Изделия, пригодные для медицинского интернета вещей, в нашей стране производятся для развитых сегментов рынка: это ЭКГ, тонометры, весы. «Домашних» приборов специального назначения, к примеру для урофлуометрии или УЗИ, пока практически нет. Но этот рынок активно формируется, и решения для него будут становиться разнообразнее.

Я считаю, что инициатива использовать устройства медицинского интернета вещей должна исходить от медицинского сообщества (пациенты в большинстве своем пассивны, потому что к этому не готовы), от образовательных и научно-исследовательских центров, где есть и ученые, и практикующие врачи, обладающие соответствующими знаниями. ИКС

Облачные провайдеры помогут в разработке блокчейн-решений

Создание, внедрение и сопровождение систем распределенного реестра – сложная работа, требующая высокой квалификации, времени и ресурсов. Снизить затраты помогут облачные провайдеры, предлагающие блокчейн-платформы по модели PaaS.

Николай Носов

Состоятельный российский клиент решил застраховать жизнь на пять лет на 120 млн руб., а выгодоприобретателем назначил свою жену. Представители организованной преступности в сговоре с коррумпированным ИТ-специалистом внесли изменения в базу данных страховой компании, и выгодоприобретателем по договору стал другой человек. Если бы не вмешательство службы безопасности, выявившей подделку, дни жизни клиента были бы сочтены.

Блокчейн нужен бизнесу

Пример с подлогом для получения страховки показывает, к каким серьезным последствиям может привести внутреннее мошенничество. «В инвестиционной сфере технологии блокчейна жизненно необходимы», – заявил генеральный директор компании «БКС Страхование жизни» Андрей Дроздов, в практике которого и произошел вышеприведенный случай.

Страховая компания начала внедрять решение для регистрации страховых договоров в распределенных реестрах. Требования конфиденциальности данных клиентов обусловили выбор в пользу приватного блокчейна. В итоге компания остановилась на open source-решении Hyperledger Fabric. В конце текущего года всем новым клиентам при получении полиса страхования будет присваиваться деперсонализированный блокчейн-идентификатор в закрытом реестре, защищающем от махинаций. В 2019 г. планируется полное внедрение системы, включающее регистрацию в блокчейне всех изменений в договорах и выплаты сумм после проверки идентификаторов клиента и выгодоприобретателя в распределенном реестре.

Хайп сделал свое дело – согласно данным Oracle, 22% ИТ-директоров предприятий уже экспериментировали с технологией распределенного реестра, а 43% планируют это сделать. Директор по развитию бизнеса компании Oracle Трасус Трасивулу выделил преимущества блокчейна – технология обеспечивает доверие, дает компаниям общую «версию правды», сокращает количество посредников, уменьшает риск человеческих ошибок (рис.1).

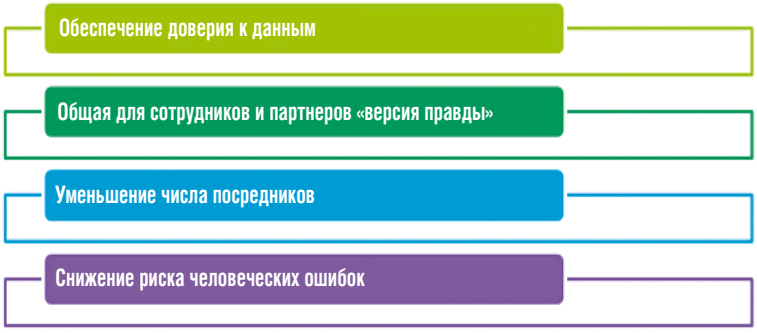
Блокчейн интересен не только финансовым организациям. Согласно отчету ученых Кембриджского университета 2017 Global Blockchain Benchmarking Study, только 30% сценариев использования технологий распределенного реестра относится к области банков и финансов (рис. 2). Этот сектор по-прежнему наиболее привлекателен с точки зрения использования блокчейн-технологий, но появляется все больше решений для государства, страховых компаний, медицины и промышленности.

Барьеры на пути использования

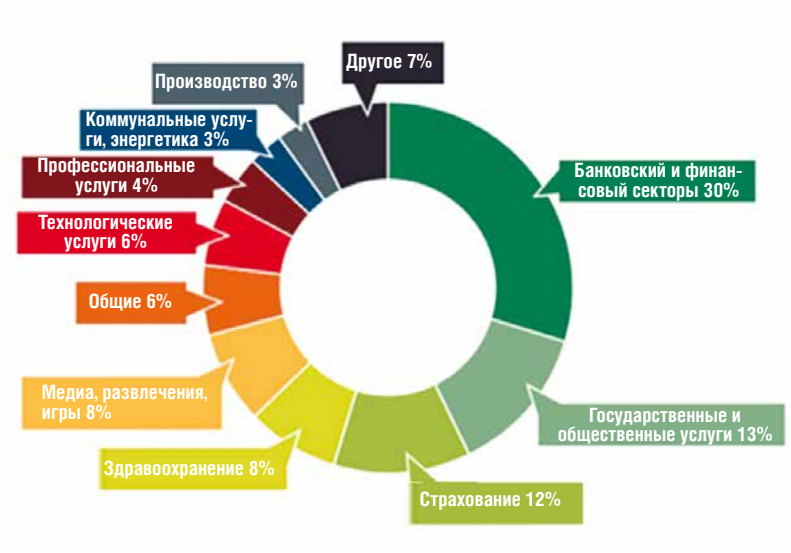
Бизнес начал понимать преимущества технологии распределенного реестра, но внедрение в промышленности пока пробуксовывает. Переход к новым технологиям всегда сталкивается с консерватизмом привыкших работать по устоявшимся правилам сотрудников и компаний, да и далеко не всем нравится действовать в условиях повышенной прозрачности, когда ничего нельзя подправить задним числом.

К этому добавляются технические трудности: развертывание решений в соответствии с существующими политиками безопасности, сложности интеграции распределенных реестров в бизнес-процессы и ИТ-инфраструктуру компаний, обеспечение эластичности и мас-

Рис. 1. Преимущества блокчейна для бизнеса



По данным Oracle



Источник: 2017 Global Blockchain Benchmarking Study

Рис. 2. Области использования технологии распределенного реестра

штабируемости решений, необходимость постоянного обновления быстро эволюционирующих блокчейн-платформ, сложность сопровождения систем.

Блокчейн как сервис

Часть проблем может решить облачный провайдер. Создание блокчейн-решений на облачной платформе дает гибкость, обеспечивает легкую масштабируемость, избавляет клиента от необходимости разбираться в тонкостях развертывания и поддержания в актуальном состоянии блокчейн-платформы, от текущих работ по резервному копированию, установке патчей, мониторингу системы и устранению сбоев на системном уровне.

Первой услуги по модели «блокчейн как сервис» предложила компания Microsoft. С осени 2015 г. Microsoft Azure открыла своим клиентам возможность использовать технологию блокчейн по модели Ethereum Blockchain as a Service (EBaaS). За первые два месяца после анонса вокруг Microsoft Azure EBaaS образовалась экосистема из десятка компаний, решения которых стали доступны другим клиентам Microsoft Azure. В 2016 г. по сервисной модели начала предоставляться платформа Emercoin.

Не отставали и конкуренты. Компания IBM в 2016 г. стала предлагать разработчикам по сервисной модели платформу Hyperledger Fabric, а в июле 2018 г. объявила о запуске платформы LedgerConnect, предназначенной для предоставления блокчейн-приложений финансовым компаниям. Партнерами IBM в этом проекте выступили американская система расчетов по валютным операциям CLS и несколько крупных банков, включая Barclays и Citigroup. Сервис построен по той же схеме, что и потребительские магазины приложений типа App Store.

Свой вариант предложила компания Amazon, открывшая доступ по сервисной модели к платформам Ethereum и Hyperledger Fabric. Компания предоставляет шаблоны AWS CloudFormation, автоматизирующие создание и настройку сетей блокчейн в сервисах Amazon Elastic Compute Cloud (EC2) или Elastic Container Service (Amazon ECS). Среди известных клиентов – немецкая компания T-Mobile, разрабатывающая платформу цифровой идентификации и аутентификации с использованием Sawtooth – технологии блокчейна, доступной в рамках проекта Intel Hyperledger. Решение включает сервисы Amazon EC2, Amazon S3, Amazon Lambda и Amazon ECS.

В апреле 2018 г. о готовности предоставлять Hyperledger Fabric из облака по сервисной модели сообщила компания Huawei, а в июле о планах запустить облачные сервисы на блокчейн-платформах Ethereum и Hyperledger Fabric объявила Google.

В конкурентную борьбу включилась компания SAP, реализовавшая в рамках SAP Cloud Platform пилотный сервис «блокчейн как услуга» и уже предложившая рынку свое ориентированное на массового пользователя блокчейн-решение TrueRec для подтверждения подлинности документов на базе платформы Ethereum. В августе 2018 г. SAP сообщила о создании нового консорциума для разработки облачных блокчейн-приложений. Это ПО предназначается для отслеживания перемещения товаров от их выпуска до поставок производителями. Клиенты SAP могут протестировать пилотный блокчейн-проект, а в дальнейшем использовать API для подключения к блокчейн-сети других решений, таких как система SAP HANA.

Возможность интеграции с уже используемыми клиентами системами – важный козырь в борьбе за потребителя блокчейн-услуг. По такому пути движется и компания Oracle, которая нынешним летом запустила Oracle Blockchain Cloud Service на базе Oracle Blockchain Cloud Platform. Помимо стандартных услуг поддержки платформы на базе Hyperledger Fabric и шаблонов разнообразных смарт-контрактов, компания предлагает API со своими и сторонними SaaS-приложениями и on-premise-системами клиента. Учитывая популярность СУБД Oracle, особый интерес представляет API с самой распространенной у заказчиков базой. При хранении «тяжелых» данных, например рентгеновских снимков, имеет смысл загружать их в СУБД Oracle, а в блокчейне хранить только хеш. При этом можно через API связывать места хранения снимков с подтверждающим их подлинность в блокчейне хешем.

Что в России?

Практически все основные мировые облачные провайдеры вышли на рынок блокчейн-услуг, но отечественные игроки не торопятся. Так что той же компании «БКС Страхование жизни» приходится работать с Oracle.

Что нормально для коммерческого сектора – совершенно не годится для государства. В рамках программы импортозамещения госсектор обязан использовать российское ПО или программы с открытым исходным кодом с соответствующими лицензиями. Кроме того, российское законодательство требует задействовать сертифицированные средства шифрования. Однако, по мнению генерального директора Центра практического применения блокчейн-технологий «Орбита» Игоря Калганова, ни одна из имеющихся блокчейн-платформ не соответствует данным требованиям.

Впрочем, работы у нас в стране ведутся. Перспективным выглядит созданная консорциумом российских банков на базе Ethereum блокчейн-платформа «Мастерчейн», в которой используется сертифицированная ФСБ российская криптография. Больше года работает так и не получившее внедрений в бизнесе полностью российское блокчейн-решение Erachain, изначально позиционировавшееся как отечественная система учета юридически значимых действий.

Идут процессы в российских госорганах. По утверждению И. Калганова, осенью в тестовую эксплуатацию на базе Минэкономразвития должна быть запущена блокчейн-система для госзакупок по закону 44-ФЗ, реализованная на платформе Corda. Электронный документ будет генерироваться для каждого действия в системе, затем подписываться электронной подписью и отправляться в хранилище. Если что-то пойдет не так – его можно использовать в суде в соответствии с российским законодательством.

■ ■ ■

Шумиха вокруг блокчейн-технологий существенно уменьшилась, но работы по созданию систем продолжаются. Разработчики могут сами разворачивать и поддерживать работоспособность блокчейн-платформ, чем они сейчас и занимаются. Но для госсектора и бизнеса, не имеющего возможности держать штат высококвалифицированных ИТ-специалистов, такие работы должны быть максимально облегчены и автоматизированы. И никуда не делись политические риски, сужающие возможности применения западных экосистем. Без российских облачных блокчейн-платформ не обойтись. Скорее всего, это понимают и наши облачные провайдеры. ИКС

Контейнеры как новый облачный тренд

Андрей Захаров, директор по продуктам и инновациям, Linxdatacenter

Контейнерная виртуализация – the next big thing в сфере облачных технологий. Почему такие гиганты, как Microsoft, Google и Amazon, инвестируют в нее, и чем эти разработки привлекают айтишников по всему миру?

Традиционная виртуализация уже не успевает за стремительным ростом рабочих нагрузок. Эмуляция физического сервера, виртуальные машины с гостевыми операционными системами, развертывание монолитных приложений в этой среде – все это представляет собой нагрузку, от которой многие компании начинают избавляться, переходя на микросервисную архитектуру и контейнеры.

Современный подход заключается в том, чтобы исключить слой эмуляции и обеспечить прямой доступ приложений ко всем необходимым ресурсам. Контейнерная виртуализация (container-based virtualization) – это в некотором роде возврат к модели мейнфреймов IBM и Sun Microsystems в новом технологическом исполнении. Одно ядро и одна ОС делятся между всеми работающими на ней приложениями. Веб-сервер, база данных, почтовый сервер, кэширующий сервер – все нужные для работы компоненты не разворачиваются в виртуальной среде, а находятся в специальных контейнерах. При таком подходе реализуется микросервисная архитектура, в которой компоненты ИТ-системы распределены и взаимодействуют друг с другом при помощи сетевых протоколов и API.

Технологии контейнеризации построены на свободном ПО. Наиболее популярный формат, ставший де-факто отраслевым стандартом, – Docker, наиболее популярная платформа – Kubernetes, оболочка для оркестрации контейнеров. Изначально решение Kubernetes использовалось для внутренних нужд Google, на рынок его вывели в 2013 г., и теперь оно свободно распространяется как для развертывания на серверных мощностях пользователей, так и в качестве сервиса из облаков Google, AWS и Microsoft Azure.

Можно выделить набор причин, которые делают микросервисную архитектуру на базе контейнеров одним из самых прорывных направлений в облачных технологиях на ближайшие годы.

Оптимизация ресурсов, скорость развертывания и масштабирование

На один физический сервер при контейнерном развертывании удается поместить в 2–3 раза больше приложений, чем при использовании классической модели виртуальных машин. Гостевые ОС не потребляют ценные ресурсы, единая платформа устраняет необходимость интеграции компонентов, не требуется резервировать запас ресурсов, все компоненты упакованы в контейнеры. Скорость развертывания из контейнеров – от нескольких секунд до минут, что в разы быстрее по сравнению с обычной виртуализацией. Размер контейнеров варьируется в пределах нескольких десятков мегабайт, что совсем немного по сравнению с виртуальными машинами минимальным размером от нескольких гигабайт.

В итоге – обслуживание большего числа обращений к системе на том же объеме «железа».

Масштабирование при контейнерном подходе происходит путем добавления физических или виртуальных нод (node), т.е. вычислительных узлов кластера. Это позволяет при необходимости заказывать увеличение объема потребляемых ресурсов с соответствующей моделью оплаты и таким образом отрабатывать пики нагрузки на ИТ-систему без капитальных затрат.

Новый уровень отказоустойчивости

В кластере контейнеры «размазываются тонким слоем» по множеству нод в рамках ИТ-системы. Ресурсы каждой ноды отслеживаются автоматически и дублируются. Если нода «вылетает», все вычисления с нее переносятся в другую область кластера. При этом с точки зрения пользователя в его работе с приложениями ничего не происходит. Для такого же уровня отказоустойчивости виртуальной машины нужно дублировать ее целиком: сервер, ОС и т.д.

Контейнеры несут в себе полноценную среду: приложение, все необходимые библиотеки, зависимые объекты и файлы настройки – все со-

брано в один пакет. За счет контейнеризации различия в ОС, конфигурациях и инфраструктуре, на которой происходит развертывание, полностью нивелируются. Таким образом контейнеры решают еще одну важную задачу – обеспечивают надежную работу бизнес-приложений при смене ими вычислительной среды.

Защита инвестиций в ИТ

Контейнерные среды нетребовательны к «железу», на котором они развертываются. Более того, если вы уже вложили средства в создание классической платформы виртуализации, то можете разместить контейнеры и поверх виртуальных машин. Такие решения предлагает, например, VMware, позволяя на кластере серверов создавать виртуальные машины, на которые надстраивается Kubernetes-среда. Это дает возможность получить работающий слой контейнеров на существующей системе.

Еще один подход предлагает на базе своих продуктов SUSE: это решение Kubernetes уровня enterprise для десятка и более вычислительных узлов. Инфраструктура строится специально под контейнеры, все задачи по ее созданию передаются в ЦОД, далее на ней разворачивается все необходимое для эксплуатации приложений в контейнерной среде. Такой подход используется главным образом для систем e-commerce, ERP, онлайн-банкинга, а также бизнес-аналитики.

В целом рост популярности и стремительное проникновение контейнеров в рабочие процессы компаний во всем мире делают вложения в эту модель ИТ-архитектуры актуальными на долгую перспективу.

Эволюция в сторону enterprise-сегмента

Контейнерные технологии присутствуют на рынке не первый год. Сегодня они приобретают универсальную актуальность и вызывают интерес как у разработчиков приложений, так и у enterprise-заказчиков. Крупный бизнес все чаще заказывает ИТ-системы у внешних разработчиков или начинает пользоваться новыми ИТ-сервисами, которые разрабатываются и запускаются на контейнерной архитектуре.

На данном этапе развития рынка контейнерную архитектуру оптимально получать «под ключ», в виде комплексной услуги, включающей серверы в ЦОДе, каналы связи и подготовленную под конкретные задачи контейнерную среду с технической и сервисной поддержкой.

С точки зрения сохранения конкурентоспособности в условиях цифровой экономики использование лучших ИТ-инструментов и адаптация к контейнерам – уже не опция, а необходимость. ИКС

ЦОД как сейф

Тарас Чирков, руководитель ЦОД Linxdatacenter в Санкт-Петербурге

Почему физическая защита дата-центров – самый важный уровень общей безопасности данных и какую роль в процессе ее обеспечения играет сегодня биометрия.

Сизифов труд?

Как ни совершенствуются инженерные системы современных ЦОДов и механизмы контроля и мониторинга, полностью избежать аварий и последующего простоя не удается. Достаточно просмотреть публикации в отраслевых СМИ на эту тему, чтобы получить подтверждение высказанного тезиса. «Падают» даже самые авторитетные частные дата-центры глобальных организаций и коммерческие ЦОДы, в которых размещается ИТ-нагрузка ведущих мировых компаний.

Причины сбоев самые разные. Рассмотрим хотя бы недавние примеры. В дата-центре Джорджтаунского университета произошел пожар, ИТ-системы учебного заведения вышли из строя, и полное восстановление всей функциональности заняло несколько дней. Сбой системы электроснабжения ЦОДа стал причиной проблем с мессенджером Telegram, а авария в дата-центре диспетчерского агентства Eurocontrol, управляющего авиасообщением в Европе, привела к многочисленным задержкам рейсов на протяжении пяти часов. Погодные аномалии вызвали сбои в работе ЦОДов Equinix, негативно отразившись на доступности ресурсов облака Amazon Web Services и связанных с ним сервисов крупных ИТ-компаний.

Причинами «падения» дата-центров оказываются и действия человека – как на стадии проектирования, так и на стадии эксплуатации. Можно вспомнить компанию OVH и ее провал с контейнерным форматом дата-центров в Европе, чисто механические казусы (рабочий киркой вывел из строя электрический кабель) или атаки хакеров.

Физика процесса

Защита сетевого периметра, каналов связи, серверного сегмента и хостов – тема для отдельной статьи. Я же хочу остановиться на обеспечении физической безопасности доступа к стойкам в залах дата-центра и на существующих стандартах и требованиях.

Исходя из своего опыта, могу сказать, что большинство клиентов, особенно из банковской сферы, приходя в ЦОД, в первую очередь смотрят на то, как организована физическая безопасность на объекте – и с точки зрения инфраструктуры, и в процедурном аспекте. Услуги ЦОДа носят комплексный, многоступенчатый характер, и уровень физической безопасности систем заказчика является в этой иерархии базовым, без которого вся система безопасности становится уязвимой. Для обеспечения физической защищенности оборудования разработан ряд стандартов, прежде всего ISO:2701 и PCI DSS, по которым дата-центры сертифицируются.

Фундаментальность аспекта физической безопасности подтверждается и высоким вниманием со стороны аудиторов заказчика. Теоретически они могут проверять все что угодно, любой аспект работы ЦОДа. Но чаще всего проверки затрагивают именно физический уровень доступа к стойкам с данными. Они спрашивают: «Как у вас работают камеры видеонаблюдения? как ведется журнал посещений? сколько уровней авторизации нужно пройти для прохода в серверный зал? как они устроены? Покажите, как будет проходить визит нашего сотрудника для техобслуживания стойки» и т.д.

Опись, протокол, отпечатки пальцев

Отмечу, что биометрические технологии контроля доступа в помещения ЦОДов, а также к отдельным стойкам с клиентским оборудованием внедряются все шире. Ведущие мировые операторы дата-центров используют решения на основе биометрии, и это не просто дань моде или формальность. Биометрия как технология сегодня достигла оптимального уровня функциональности при доступной стоимости, так что высокий спрос объясним.

> Большинство клиентов, особенно из банковской сферы, приходя в ЦОД, в первую очередь смотрят на то, как организована физическая безопасность на объекте.

Если учесть, что обычно в число клиентов коммерческого дата-центра входят компании из сферы финансовых услуг, здравоохранения и промышленности, а также транспортные, торговые и энергетические компании, максимально требовательные к уровню защиты информации, то характеристику «излишний» к понятию «уровень физической защиты данных в ЦОДе» применить нельзя.

Аналитическая компания Markets & Markets оценивает общий объем рынка систем контроля доступа в ЦОДы в 2018 г. в $13,77 млрд. Логическая и сетевая безопасность на уровне DNS/SSL и физическая безопасность данных, которую обеспечивают видеонаблюдение и биометрический контроль, играют сегодня важнейшую роль в стратегии интегрированного подхода к целостности данных.

Технологии предлагают широкий выбор биометрических инструментов контроля и идентификации. Самой зрелой признается авторизация по отпечатку пальца, проводятся эксперименты в направлении распознавания радужной оболоч-

Ключница, предоставляющая ключи к стойкам с оборудованием по отпечатку пальца и карте

ки глаза, сканирования запястья руки и даже индивидуального запаха человека. Сканирование глаза переходит от радужки к распознаванию структуры кровеносных сосудов в глазном яблоке. По оценкам Gartner, рост общего объема использования биометрической авторизации с помощью мобильных инструментов с 2014 по 2016 гг. составил 25%. Темпы развития этого направления Markets & Markets оценивает в 9,6%. Основной тренд сегодня – использование биометрии в банковских приложениях, а также компаниями, работающими с данными, которые имеют высокий уровень важности и составляют коммерческую тайну. Распознавание лиц также перешло в стадию коммерческой эксплуатации, но в дата-центрах эта технология не так популярна, поскольку существует ряд стратегий фальсификации для ее обхода.

> Видеонаблюдение и биометрический контроль играют сегодня важнейшую роль в стратегии интегрированного подхода к целостности данных.

Следующим этапом после сканирования отпечатков пальцев станет скан венограммы запястья (расположение вен так же уникально, как и отпечатков пальца, но быстрее и проще верифицируется).

Инсайдер неизбежен?

Сегодня доступен широкий спектр решений для обеспечения физической защиты данных.

Во-первых, это размещение оборудования клиентов внутри защищенного периметра с отдельным доступом к нему. Ограждение устанавливается от потолка до самого пола (ниже уровня фальшпола), на входе в огороженный периметр проводится дополнительная аутентификация по отпечатку пальца и используются отдельные ключи. В некоторых случаях организуется допуск с одновременной биометрической авторизацией двух человек. Таким образом вероятность инсайда уменьшается в разы, поскольку подкуп или внезапный нервный срыв сразу у двух ключевых сотрудников заказчика или персонала ЦОДа практически исключен.

Во-вторых, применяются решения для точечной защиты в рамках многоуровневой архитектуры безопасности доступа. Вход в дата-центр, доступ на этаж, доступ в серверную комнату и, наконец, доступ к нужной стойке – все это можно надежно спрятать за «забором» из нескольких этапов биометрической авторизации по сквозному принципу от шлагбаума до стойки.

Но развиваются не только технологии защиты, но и технологии взлома, кражи и неправомерного доступа к информации. В 2016 г. был поставлен новый рекорд темпов роста числа инцидентов класса «кража личности» (identity theft) в США с показателем более 1000 эпизодов (данные Identity Theft Resource Center). По состоянию на осень 2018 г. зафиксировано 668 таких эпизодов. В масштабах планеты, по оценкам компании Cifras, в 2017 г. произошло 174 523 подобных инцидента (рост 152% за последние 10 лет). Сведения о 1093 масштабных инцидентах, связанных с нарушением защиты данных, просочились в СМИ. 2017 г. также запомнился всплеском кейсов ransom-ware в мае и июне, причем среди пострадавших компаний были FedEx, Telefónica, Deutsche Bahn и британская система здравоохранения (UK National Health Services).

Биометрия не остается в стороне от прогресса инсайдерских технологий, так как эти решения реализуются на базе цифровых инструментов и полностью автоматизированы. Многое зависит от качества оборудования для захвата и верификации биометрии и способа хранения этих данных. В частности, большинство современных систем использует одностороннее шифрование для защиты биометрических идентификаторов, чтобы, украв цифровую копию биометрической информации пользователя, злоумышленники не могли бы воссоздать оригинал. Такой биометрический шаблон может быть скомпрометирован в месте своего хранения в случае ненадлежащего

режима безопасности на объекте. И здесь мы снова видим, что базовая физическая безопасность и защищенность объекта становятся важнейшим уровнем общей безопасности данных. То, как биометрические шаблоны используются мошенниками, определяет степень причиненного ущерба – украденные данные могут служить для реконструкции биометрических паттернов или создания физической копии. Поэтому второй важнейший уровень безопасности – такое шифрование шаблона, которое гарантировало бы, что, оказавшись в руках преступников, он будет для них бесполезен. Сам шаблон должен быть достаточно защищен, чтобы не нести в себе опцию неправомочного использования.

Инсайдеры и «человеческий фактор» среди сотрудников

Причина внедрения биометрических инструментов контроля доступа в Linxdatacenter – борьба с нарушениями использования личных карт доступа, введенных на первом этапе организации системы контроля. В некоторых случаях карты передавались третьему лицу (сотрудник забыл дома свою, а выйти/зайти нужно), что привело к недопустимому повышению роли человеческого фактора в процессе, так как персонал службы охраны выявлял нарушителей по несовпадению изображения с видеокамер и фотографии владельца карты в СКУД. Введение системы сканирования отпечатков пальцев сотрудников решило эту проблему. Биометрическая аутентификация стала параллельным инструментом подтверждения личности наряду с визуальной идентификацией и проверкой документов. Со своей задачей сканирование пальца справилось, security-инциденты из нашей практики почти полностью исчезли.

Сканер отпечатков пальцев

Да, ни одно биометрическое решение не защищает на 100% от инсайдерской деятельности: можно подкупить электрика, он пойдет и выключит ввод, дата-центр «упадет». Построить бизнес ЦОДа по модели, при которой отдельный сотрудник не способен причинить критический ущерб, можно, но обычно за счет удобства реализации бизнес-процессов для клиентов. В этом плане биометрия нам только помогает: после тестового периода биометрического доступа для сотрудников мы начали использовать эту систему для постоянных посетителей дата-центра – человек регистрируется в системе по документам, передает нам свои биометрические данные (отпечаток пальца), и при повторных посещениях для прохода в ЦОД ему достаточно подтверждения аутентичности отпечатков. Для нас – безопасно, для клиентов – удобно, поскольку не требуется носить и предъявлять документы, удостоверяющие личность. Для разовых посещений реализована система электронной регистрации визитов, значительно упростившая ведение и отслеживание архива посещений.

Высокие технологии – высокие риски?

Там, где технологии упрощают жизнь, они же обычно ее и усложняют – просто в другом срезе. С надежностью биометрической идентификации все усложняется, к примеру, с точки зрения возможности компрометации. Так, если компрометируются пароли от аккаунтов, то пользователи оповещаются и пароли меняются. Аналогичные утечки биометрических идентификаторов пользователей могут привести к необратимым последствиям, поэтому безопасное хранение этих данных играет ключевую роль.

В Linxdatacenter уровень безопасности и качество работы СКУД подтверждены аттестацией на соответствие требованиям ФСТЭК по хранению персональных данных. Когда речь заходит о биометрии, важность подобного рода сертификации сложно переоценить.

Популярность биометрии растет, но ее дальнейшая судьба будет зависеть от того, насколько разработчики решений смогут избежать громких инцидентов с утечками и взломами при сохранении удобства и надежности в использовании. Мы в Linxdatacenter реализовали решение на биометрии в узком нишевом ключе и пока можем говорить только о плюсах проекта. ИКС

Что угрожает безопасности ЦОДа?

Эмоциональная дискуссия «Как обеспечить безопасность ЦОДа?» на круглом столе конференции «ЦОД-2018», организованной «ИКС-Медиа», показала, что мнения по этому вопросу расходятся.

Николай Носов

Инженерные системы ЦОДов становятся сегодня все более «умными» и начинают представлять интерес для злоумышленников. Поэтому, как указал Андрей Ивашов, руководитель по развитию направления DCIM подразделения IT Division компании Schneider Electric, риски, связанные с инженерной инфраструктурой, следует рассматривать в модели угроз.

Еще одна проблема, которая возникнет в недалеком будущем, – безопасность Edge-устройств. Сегодня ею в нашей стране практически не занимаются, но, по мнению А. Ивашова, развитие интернета вещей заставит обратить на безопасность периферийных вычислений серьезное внимание. Например, когда страховым компаниям понадобится оперативная обработка видеопотока высокого качества с видеорегистраторов автомобилей, появятся удаленные вычислительные системы – «щупальца» из ЦОДов. А значит, появится потребность в обеспечении их безопасности.

Андрей Ивашов

> Системы управления кондиционированием и электропитанием ЦОДа все чаще имеют доступ к интернету и подключение к информационной сети ЦОДа. Появляются новые возможности для кибератак, на которые специалисты по информационной безопасности не обращают внимания».

Внешняя атака на ЦОД через «умную» инфраструктуру – пока вопрос больше теоретический. Знать о такой возможности надо, но практики озабочены скорее другими проблемами. «Следует исходить из оценки рисков для каждой конкретной компании», – подчеркивает заместитель генерального директора по ИТ Вологодской сбытовой компании Владимир Гайлит. 80% проблем безопасности обусловлены внутренними проблемами компании. Риски внутренних утечек данных значительно выше, чем риски внешних атак, во всяком случае для распределенной сети дата-центров энергетиков. Хотя, если судить по многочисленным сообщениям СМИ об утечках данных из западных ЦОДов, проникновение злоумышленников из интернета в ЦОД может фатально сказаться на бизнесе компании.

Для гарантированной бесперебойной работы ЦОДа недостаточно физической охраны периметра и резервирования инженерных систем. «Нет ни одного телеком-оператора, у которого машзал находился бы в комнате безопасности. Что будет с дата-центром, если в соседнем помещении начнется пожар? Об этом мало кто задумывается в нашей стране», – отмечает Александр Нилов, старший менеджер по продукции для ИТ-инфраструктуры компании Rittal. Например, в Германии, по его словам, все крупные телеком-операторы используют для физической защиты ЦОДов или машзалов комнаты безопасности. В этой стране жесткое законодательство по защите данных, которое непосредственно регулирует ситуации их потери,

например, физического уничтожения. Может быть, стоит задуматься о нормативном регулировании безопасности ЦОДов и в нашей стране? Или заняться безопасностью ЦОДов в рамках разрабатываемых стандартов программы «Цифровая экономика»?

Дата-центры, имеющие физическую защиту от внешних взрывов и пожаров, в России, конечно, есть, например, в оборонной отрасли, энергетике, нефтехимической промышленности и т.п. По словам заместителя гендиректора по системной интеграции и кибербезопасности Московского завода «Физприбор» Вадима Подольного, защищенные помещения используются для размещения оборудования АСУ ТП атомных станций.

Согласно Общим правилам взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств, выпущенным Ростехнадзором еще шесть лет назад, на новостроящихся объектах оборудование, которое управляет технологическими процессами, должно иметь физическую защиту от внешних взрывов и пожаров. Требования зачастую реализуют, размещая оборудование в цокольном этаже с толстыми стенами, но, как указывает А. Нилов, это не всегда можно сделать. Так что у поставщиков сейфов для ИТ-оборудования и различных комнат безопасности рынок есть.

Сегодня в профессиональном сообществе активно обсуждается закон о безопасности КИИ. По мнению В. Подольного, серьезно наказывать за неисполнение законодательства по КИИ будут в только случае возникновения соответствующих инцидентов. Главное – обеспечивать не «бумажную», а реальную безопасность, чтобы такие случаи не произошли. Тогда и проблем с регуляторами не будет.

Возможно, вендоры систем безопасности преувеличивают размер дополнительных затрат, которые потребуются на соблюдение требований регулятора, но практика показывает, что проверки выполнения требований по информационной безопасности, в том числе закона о защите персональных данных, проводятся. Как правило, проверяющие не являются специалистами по ИБ и подходят к вопросу формально, запрашивая подтверждающие сертификаты и другие документы. Так что и у «бумажных безопасников» фронт работ есть.

> Базой всего является физическая безопасность. Ее обеспечить довольно просто. Если не считать пожары, серьезных инцидентов в России не припомню. Если говорить об информационной безопасности, то основной упор должен делаться на сетевой безопасности.

Сергей Мищук

Был период, когда профессионалы дискутировали, законна или незаконна криптография, в том числе и в Windows, не сертифицированная ФСБ. Потом рынок был взбудоражен законом «О персональных данных». Говорили, что никто не сможет удовлетворить требования регуляторов и нужно прекращать операционную деятельность. В таком же состоянии сейчас находится ситуация с КИИ.

> В Европе многие ЦОДы имеют страховку от различных рисков. В России таких не знаю».

Александр Нилов

По мнению технического директора DataLine Сергея Мищука, никто из регуляторов в здравом уме не станет заниматься вредительством и «убивать» рынок. В обозримом будущем ситуация утрясется, и станет понятно, что можно и чего нельзя делать. Пока же следует придерживаться прагматической позиции – не подставляться. ИКС

Мобильное приложение для общения с сотрудниками вне офиса

Компания Panasonic вывела на рынок фирменное мобильное приложение Mobile Softphone, которое поддерживает как аудио-, так и видеозвонки со смартфона. Во втором случае изображение пользователя передается либо на устройство другого абонента Mobile Softphone, либо на SIP-видеотелефон Panasonic KX-HDV430RU. Изображение с коммуникационной IP-камеры Panasonic KX-NTV150 или IP-видеодомофона Panasonic KX-NTV160 также может передаваться на смартфон пользователя приложения.

Приложение совместимо с мобильными операционными системами iOS v.10 и выше, а также Android v.4.4 и выше. Его можно бесплатно скачать в App Store и Google Play. Интерфейс приложения полностью русифицирован.

В аппаратной части продукт совместим с IP-АТС Panasonic KX-NS500RU, KX-NS1000RU, KX-NSX1000RU/KX-NSX2000RU, KX-HTS824RU. Благодаря функции MRG (Media Relay Gateway) в IP-АТС серий KX-NS/NSX удаленные пользователи подключаются к офисной АТС без какого-либо дополнительного оборудования для создания VPN.

В настройках приложения можно задать два IP-адреса АТС – глобальный и локальный. Это позволяет использовать приложение как внутри офиса (при подключении к локальной Wi-Fi-сети), так и вне его – через любой интернет-канал.

Если во время разговора через Mobile Softphone поступает входящий GSM-вызов, то при ответе на него приложение автоматически переводит текущий звонок в режим удержания. В процессе разговора также доступны функции удержания и перевода вызова. Приложение Mobile Softphone поддерживает функцию push-уведомлений, что позволяет использовать приложение в фоновом режиме и существенно экономит расход аккумулятора.

Безопасность соединений через Mobile Softphone обеспечивается поддержкой функции SIP-TLS (Transport Layer Security).

Возможность использования приложения открывается для абонентов IP-АТС Panasonic с помощью ключей активации на станции. Клиент приобретает ключ активации на необходимое число пользователей и при необходимости может расширить количество пользователей, докупив дополнительные ключи.

www.panasonic.com

Трехфазные ИБП с высокой плотностью мощности

Компания CyberPower выпустила серию трехфазных источников бесперебойного питания с высокой перегрузочной способностью, получившую название HSTP. ИБП предназначены для обеспечения бесперебойного электропитания критически важных систем в центрах обработки данных, финансовых структурах, медицинских организациях, промышленных предприятиях, на транспортных узлах, в ситуационных центрах и т.д.

Серия HSTP представлена моноблочными моделями мощностью 10–500 кВА с возможностью параллельного подключения до восьми устройств. ИБП построены по принципу двойного преобразования энергии и имеют три фазы на выходе и три фазы на входе.

Все модели серии поддерживают работу с внешними батарейными массивами, что позволяет гибко подходить к обеспечению объекта нужным временем автономии. Кроме того, реализована адаптивная работа в паре с генераторными установками, что еще больше увеличивает время автономной работы защищаемого оборудования или объекта.

ИБП серии HSTP относятся к оборудованию с высокой плотностью мощности. Высокие показатели обеспечиваются современной элементной базой, в частности, управлением центральным микропроцессором и работой силовых IGBT-транзисторов, благодаря чему форма выходной синусоиды имеет минимальные искажения. Показатели КПД в серии HSTP достигают 96% в нормальном режиме и 98% в ECO-режиме. ИБП имеют независимое зарядное устройство, порт аварийного отключения EPO, функции интеллектуального управления зарядом батарей, поддерживают «холодный» старт, а также возможность резервирования N + 1 и N + N.

Производитель обеспечивает серию ИБП HSTP четырехлетней гарантией в штатном режиме.

www.cyberpower.com

Трехфазные ИБП для защиты критически важного оборудования

Компания Tripp Lite представила на российском рынке трехфазную систему ИБП SmartOnline S3MX, предназначенных для обеспечения бесперебойного электропитания критически важных систем в таких областях, как дата-центры, корпоративные сети, системы безопасности, аварийные службы, финансовые организации, предприятия розничной торговли, транспорт, а также промышленные предприятия и телекоммуникации. ИБП серии S3MX имеют мощность 30–200 кВА с возможностью параллельного подключения для наращивания мощности (до 400 кВА) или резервирования.

ИБП Tripp Lite линейки SmartOnline S3MX обладают КПД до 98% и компактными габаритами. Низкий коэффициент гармонических искажений на входе THDi (<3%) позволяет исключить дополнительные расходы, связанные с вынужденным завышением мощности генераторов и другого оборудования, а низкий коэффициент искажений напряжения на выходе THDv (≤ 2%) и коррекция коэффициента активной мощности повышают производительность и совместимость с разными типами нагрузки.

Сенсорный экран с диагональю 25,4 см / 10” (для моделей мощностью от 100 кВА) обеспечивает полноценное локальное управление посредством интуитивно понятного интерфейса с расширенным функционалом. Он отображает критически важные рабочие режимы и диагностические параметры: уровни нагрузки, запас времени работы, состояние аварийной сигнализации, уровень заряда батарей и значения напряжения и частоты. Опциональная карта сетевого управления WEBCARDLX и бесплатное программное обеспечение предоставляют возможность дистанционного управления и контроля параметров посредством веб-интерфейса, SSH/telnet и SNMP, а также интеграции с широким спектром систем сетевого администрирования и платформ управления инфраструктурой ЦОДа.

www.tripplite.com

Аккумуляторы для тяжелых условий эксплуатации

Компания GNB Industrial Power, подразделение концерна Exide Technologies, представила аккумуляторы PowerCycle PC12/180 FT для тяжелых условий эксплуатации. Аккумуляторы изготовлены по технологии dryfit, в соответствии с которой в устройствах используется электролит, загущенный до желеобразного состояния, что исключает его вытекание при эксплуатации и транспортировке. Большой запас электролита обеспечивает высокий циклический ресурс (1600 циклов заряд-разряд), а также высокую теплоемкость аккумуляторов. Это гарантирует отсутствие эффекта термического разгона и надежную работу в сложных температурных условиях: диапазон рабочих температур составляет от –40°C до +55°C. Клапаны избыточного давления, предусмотренные конструкцией аккумулятора, поддерживают внутри корпуса необходимое давление для протекания реакции рекомбинации кислорода и водорода с образованием молекул воды, в связи с чем аккумуляторы PowerCycle не требуют долива воды на протяжении всего срока эксплуатации, а также характеризуются низким газовыделением. Для размещения аккумуляторов не требуется специальное помещение. Устройства устойчивы к глубокому разряду, способны работать в условиях недозаряда и быстро восстанавливают номинальную емкость, что важно для объектов с ненадежным энергоснабжением.

Номинальное напряжение аккумуляторов PowerCycle PC12/180 FT составляет 12 В, номинальная емкость – 180 Ач; габариты (Д х Ш х В) – 568 х 128 х 320 мм; вес – 58,4 кг; срок службы – 20 лет (при 20°C).

Выводы аккумуляторов расположены на фронтальной поверхности, что позволяет устанавливать их в телекоммуникационные шкафы и стойки, а также облегчает монтаж и обслуживание.

На аккумуляторы PowerCycle оформлены все необходимые сертификаты и разрешения для эксплуатации на территории РФ, включая декларации Федерального агентства связи, а также декларации и сертификаты ГОСТ Р.

www.akku-vertrieb.ru

РЕКЛАМА В НОМЕРЕ

ХАЙРЕФ РУС
Тел/факс: (495) 225-4892
www.hiref.it/ru . . . . . **с. 44–45, 4-я обл.**

DATASPACE
Тел.: (495) 663-6564
Факс: (495) 663-6802
E-mail: info@dataspace.ru
www.dataspace.ru . . . . . **1-я обл, с. 36–37**

GREENBUSHDC
Тел.: (800) 350-1500
www.greendc.ru . . . . . **с. 60–61**

ITK
Тел.: (495) 542-2222
Факс: (495) 542-2224
E-mail: info@itk-group.ru
www.itk-group.ru . . . . . **с. 15**

PANASONIC
Тел.: (495) 665-4292
E-mail: office@panasonic.ru
www.panasonic.ru . . . . . **с. 7**

RITTAL
Тел.: (495) 775-0230
Факс: (495) 775-0239
E-mail: info@rittal.ru
www.rittal.ru . . . . . **с. 13, 43, 54–55**

SCHNEIDER ELECTRIC
Тел.: (495) 777-9990
Факс: (495) 777-9992
www.schneider-electric.com. . . . . . **с. 50–51**

Указатель фирм и организаций

ABB **21, 45**
Alibaba **64**
Amazon **84, 86, 89**
AMD **64**
ASHRAE **46**
Barclays **84**
Bitzer **45**
Bosch SI **21**
Cabero **34, 46**
Carel **45**
China Unicom **6**
Cisco **22, 37, 63**
Citigroup **84**
Citrix **12, 58**
CLS **84**
CyberPower Systems . . . **33,** **34, 94**
Daichi **34**
Danfoss **45**
DataCenter Dynamics . . . **55**
DataLine **93**
DataSpace **28, 37**
Dell EMC **58, 63**
Deutsche Bahn **90**
Drees & Sommer **27**
ebmpapst **45**
Edge Computing Consortium **64**
Emerson **32**
Equinix **89**
Eurocontrol **89**
Exide Technologies **95**
Facebook **47**
FedEx **90**
Fujitsu **12**
Gartner **62, 64, 80, 90**
General Electric **21, 22**
GNB Industrial Power . . . **95**
Google **12, 86**
GreenBush DC **60, 61**
Hana Financial Group . . . **12**
Heavy Reading **66**
HiRef **33, 44, 45**
Hitachi **21, 21**
Honeywell **21**
HP **37, 58**
HPE **12, 62**
HTS **35**
Huawei **59, 84**
IBM **21, 84, 86**
IEEE **67, 70, 71**
iKS-Consulting . . . . **4, 9, 10,** **19, 57**
Intel **63, 64**
INVITRO **78**
IoT Analytics **21**
IXcellerate **6**
KEHUA Tech **31, 32**
Lattelecom **46**
Leviton **68**
Light Reading **66**
Linxdatacenter . . **86, 88, 91**
Markets & Markets . . **89, 90**
Mellanox Technologies . . **68**
Microsoft . . **12, 22, 50, 57,** **59, 84, 86**
Molex MPN Structured Cabling **67**
MTU **34**
Netflix **52**
NEXTDC **12**
Nutanix **58, 64**
ONDOC **15, 82**
Oracle . **21, 59, 83, 84, 85**
OVH **89**
Panasonic **94**
Parallels **58**
Philips Lighting **21, 22**
PIARC **20**
Piller **11**
Platinum Equity **32**
profITcool **34**
PTC **21**
Rackspace **12**
Red Hat **59**
Rightech **21, 22**
Rittal . . . . . **5, 11, 31, 54,** **55, 64, 92**
SafeDATA **35**
Samsung **21**
SAP **84**
Schneider Electric . . **5, 21,** **50, 51, 64, 92**
Siemens **21, 45**
Signify **21**
Softline **22**
Software AG **21**
STULZ **35**
Sun Microsystems **86**
SUSE **12, 87**
Telefonica **90**
The Register **47**
Tibbo Systems **22**
T-Mobile **84**
Trippe Manufacturing Company **31, 95**
UK National Health Services **90**
Uptime Institute . . . **12, 34,** **37, 55**
USM Group **22**
Vertiv **32**
VMware . . **12, 57, 59, 87**
Ziehl-abegg **45**
«Абитех» **31**
«Авантаж» **33**
«АйТи Энергофинанс» . . **22**
ГК «АйТи» **21**
Американский совет по зеленому строительству . **25, 26**
«Амнисс» **15**
АНО «НИИУРС» **24**
Инновационный центр «Баррикады» **59**
«Билайн» **22**
«БКС Страхование жизни» **83, 85**
«Военторг» **36**
Вологодская сбытовая компания **92**
Всемирная организация здравоохранения **82**
ВТБ-24 . . . . . **58**
«Газпром» **36**
Газпромбанк **22, 37**
Гематологический научный центр РАМН **78**
«ДатаДом» **38**
Джорджтаунский университет **89**
ДКС **6, 32, 33**
«ИКС-Медиа» . . . . **4, 31,** **67, 92**
Институт цифровой медицины **74**
«Инфосистемы Джет» . . **52**
«ИРЭ-Полюс» **65**
«К+31» **82**
«Криогенмаш» **22**
КРОК **23, 34**
«Литвинчук маркетинг» . **33**
«Мать и дитя» **79**
«Мегафон» **22**
ГК «Медси» **80**
Международная комиссия ООН по окружающей среде и развитию **23**
Международный олимпийский комитет **23**
«Мечел» **36**
Минздрав России . **74, 76,** **77, 78, 80, 82**
Министерство цифрового развития, связи и массовых коммуникаций РФ . . . **10**
Министерство экономического развития РФ . **4, 36, 85**
Минпромторг России . . **37**
«Мираторг» **36**
МТС **22, 80**
«МТУ Рус» **34**
МТУСИ **69**
«МФ Технологии» **22**
Немецкий совет по устойчивому строительству . . **26**
НИИ урологии и интервенционной радиологии им. Н.А. Лопаткина . **74, 81**
НИУ ВШЭ **74, 79**
«Новатэк» **36**
Одесская академия холода **46**
ОМЗ **36**
Центр практического применения блокчейн-технологий «Орбита» . . **85**
«Первая грузовая компания» **35**
Первый МГМУ им. И.М. Сеченова . . . **74**
«Петер-Сервис» **22**
ГК «Пожтехника» **35**
«Рассвет» **14**
ГК «Ренова» **22**
«Рефкул» **44, 45**
РНИМУ им. Н.И. Пирогова . **75, 76**
«Роснефть» **22**
«Росплатформа» **58**
Российская гильдия управляющих и девелоперов . **23**
Росстат **19**
«Ростелеком» **8**
«Ростелеком-ЦОД» . **4, 6, 9**
«Ростех» **22**
Ростехнадзор **93**
Ространспорт **20**
«Росэнергоатом» **8**
Сбербанк **33**
«Семейная» **14**
«Сервионика» **59**
ИК «Сибинтек» **22**
ИЦ «Станкосервис» . . . **22**
ГК «ТЕРМОКУЛ» **33**
«ТрастИнфо» **59**
«Уралмаш» **36**
Федеральное агентство связи **95**
Московский завод «Физприбор» **93**
ФИФА **23**
ФОМС **76**
ФСБ **85, 93**
ФСК **8**
ФСТЭК . . . **59, 80, 82, 91**
«Хайреф Рус» **45**
«Цифра» **22**
ЦНИИОИЗ МЗ РФ . . **75, 76**
«Чайка» **14**
Чайнасельхозбанк **6**
«ЭР-Телеком» **22**
ЭТП ГПБ **36, 37**

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.

TELECOM & MEDIA
CSTB

ВЫСТАВКА-ФОРУМ
29–31 ЯНВАРЯ 2019
Москва, Крокус Экспо

В ПРОГРАММЕ:

Международный форум CSTB. Telecom & Media

10-я Национальная Премия «Большая Цифра»

Специальная экспозиция OTT FUTURE

18+

Организатор
MIDEXPO
МЕЖДУНАРОДНЫЕ ВЫСТАВКИ И ЯРМАРКИ

При поддержке
Минкомсвязь России

Стратегический партнер
ТРИКОЛОР

Генеральный отраслевой интернет-партнер
COMNEWS

WWW.CSTB.RU

HiRef®

ITALIAN COOLING SOLUTIONS

ПРЕОДОЛЕВАЯ ГРАНИЦЫ

СДЕЛАНО В РОССИИ!

hiref.it/ru

Hiref Rus

Подробнее на **стр. 44**