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

ИнформКурьер-Связь

ИКС

издается с 1992 года

№ 1 2018

Edge Computing: из облаков на землю

DCDE FORUM

ИКС МЕДИА

6-я международная конференция

DATA CENTER DESIGN & ENGINEERING

26 апреля 2018 • Москва • Центр Digital October

www.dcdeforum.ru

За дополнительной информацией обращайтесь по телефонам: (495) 150-6424, 229-4978, 785-1490

Спонсоры и партнеры

RITTAL Life Is On Schneider Electric PILLER Power Systems AVANTAGE ЦЕНТР ОБРАБОТКИ ДАННЫХ LEVITON EATON Powering Business Worldwide RCNTEC

PROF IT COOL CABERO HEAT EXCHANGER HUBER+SUHNER ENERGO Группа Компаний ПОЖТЕХНИКА HITZINGER Power. Anytime. Anywhere.

HITEC Power Protection socomec Innovative Power Solutions ПРЕОРА СЭ SOLUTIONS КАЧЕСТВЕННО.СДЕЛАНО.В РОССИИ. ИМПУЛЬС ИСТОЧНИКИ БЕСПЕРЕБОЙНОГО ПИТАНИЯ ХАЙТЕД МАКСИМУМ ЭНЕРГИИ

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, Г.Ф. Куликова, Н.В. Носов

Корректор
Е.А. Краснушкина

Дизайн и верстка
Д.А. Поддъяков

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:
127254, Москва,
Огородный пр-д, д. 5, стр. 3
Тел.: (495) 150-6424, 785-1490, 229-4978.
E-mail: iks@iks-media.ru
Адрес в Интернете: www.iksmedia.ru
Тел.: (495) 502-5080
№1/2018 подписан в печать 06.04.18.
Тираж 8 000 экз. Свободная цена.
Формат 64x84/8

ISSN 0869-7973

12+

Девять лет спустя

Наш мир развивается по спирали. И информационные технологии не исключение. От централизованной обработки информации на базе мейнфреймов, которые господствовали в 70-х годах прошлого века, индустрия к концу 80-х постепенно перешла к распределенным системам на базе ПК, объединенных вычислительными сетями. Затем, с начала нынешнего века, пришло время массового объединения ИТ-активов в центрах обработки данных. Несомненные экономические преимущества такой централизации определили приоритет этой тенденции почти на два десятилетия. И вот очередной виток спирали: резкий рост интереса к распределенным граничным вычислениям – Edge Computing. О причинах и следствиях этого явления – главный материал номера.

Если «Эдж» – «горячий» ИТ-термин для всего мира, то в России не менее актуален и другой термин – «КИИ», критическая информационная инфраструктура. Одна из благих целей законодательных инициатив государства в области КИИ – вывести действительно важные для страны информационные системы из «подвалов и сараев» в надежные дата-центры. Но «дьявол в деталях»: как будут классифицироваться ИТ-объекты, по каким правилам сертифицироваться и т.д. и т.п. Хочется надеяться, что принятые правила игры будут способствовать развитию отечественной ИТ-индустрии (а не тормозить его). Мы будем самым подробным образом информировать читателей о том, как будут разворачиваться события вокруг КИИ.

Но возвращусь к спирали. На этот раз личной. Я вернулся в ИКС спустя девять лет. В совсем другой ИКС. Девять лет назад на рынке ИКС был известен в первую очередь как журналистский проект – отраслевое телеком-издание. Сегодня для большинства специалистов ИКС – это авторитетные мероприятия, консалтинг и аналитика по таким направлениям, как ЦОДы, облака, цифровая трансформация, в том числе трансформация того же телекома. Пришло время менять и контентные площадки ИКСа с учетом новых требований потребителей информационных ресурсов. Сегодня важно не только отражать текущие события и тренды, но и проводить их профессиональный анализ, уделять больше внимания практическим аспектам реализации проектов...

Если верить в теорию спирали, то и интерес к печатным СМИ должен вот-вот возродиться. Постараемся приблизить этот момент. Ну а кто отказался «от печати» навсегда или думает, что навсегда, – добро пожаловать на IKSMEDIA.RU.

Удачи на новом витке,
Александр Барсков

с. 4

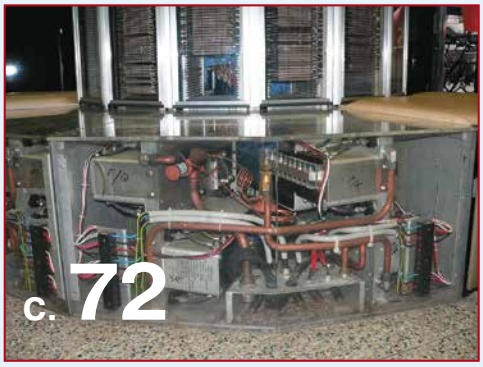
Гамбургский счет: итоги премии DC AWARDS 2017

с. 30

Е. Ягнятинский. Save to reinvest как стратегия успешного развития

с. 36

Н. Носов. Edge Computing: из облаков на землю



А. Эрлих. Двадцать тысяч лет под водой, или Особенности погружных систем

с. 76

Г. Куликова. Смартфон станет главным медицинским гаджетом?

С. Орлов.

с. 82

Гамбургский счет: итоги премии DC AWARDS 2017

В номинации «Проект года» профессиональной премии Russian Data Center Awards победителем стал мегаЦОД Сбербанка в Сколково.

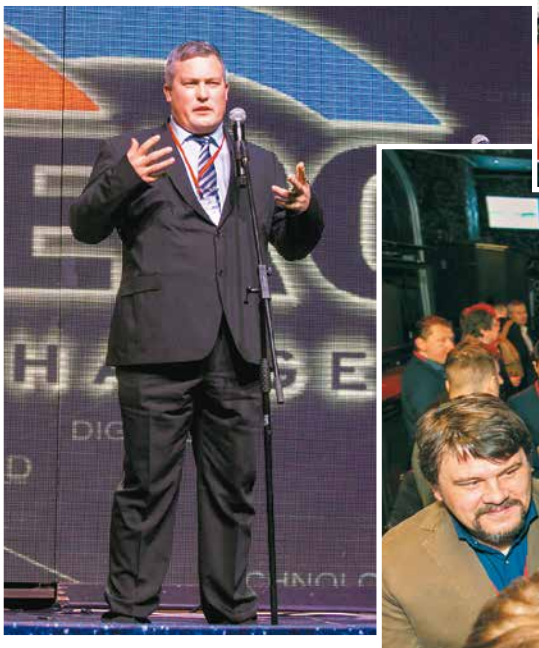
Победа совместного проекта Сбербанка, «СБ Девелопмент» и компании «Инсистемс» была ожидаемой и вполне заслуженной. Хотя в заявках на участие в конкурсе не указывались названия компаний, но членам жюри трудно было не заметить размаха проекта мегаЦОДа «Сколково» и использования в нем новых инженерных и технологических решений (подробнее об этом проекте → см. с. 6).

Церемония награждения победителей прошла в московском ночном клубе Icon, куда съехались представители отрасли дата-центров из разных уголков страны. На конкурс было подано 23 заявки, в состав жюри вошло 23 эксперта. Профессионалы оценивали профессионалов. Никакого маркетинга, только сухие цифры анонимных описаний проектов, своего рода гамбургский счет.

Помимо главной номинации – «Проект года», премии присуждались еще по семи номинациям.

В номинации «Комплексное решение ИТ + инженерная инфраструктура (комплексный проект создания инженерной инфраструктуры для решений высокой плотности для облачных сервисов и высокопроизводительных вычислений)» победила компания «Яндекс» с проектом «Владимирский ЦОД компании Яндекс». Немногие эксперты, побывавшие в этом закрытом для широкой публики дата-центре, отмечали уникальность используемых компанией современных решений. В этой номинации с российским транснациональным гигантом конкурировал проект «ЦОД для многофункционального миграционного центра» компании «Стэп Лоджик».

Дата-центры высокой заводской готовности – тема горячо и активно обсуждаемая, в том числе и на страницах журнала «ИКС» (см. № 7–8'2017, с. 24). Это внимание к prefab-ЦОДам со стороны профессионального сообще-



ства, возможно, повлияло на выбор жюри – в номинации «Лучшее решение для ЦОДа на базе отечественных продуктов» победило модульное решение петербургской компании GreenMDC, представившей проект «Создание дата-центра для размещения вычислительного кластера научно-производственной компании». Конкуренцию ему составляли проекты «Крымский республиканский ЦОД», выполненный компанией C3 Solutions, «Модульный ЦОД для Красноярской ГЭС» компании «ЛАНИТ-Сибирь» и центр исполнения заказов интернет-магазина «Юлмарт».

Безальтернативным стал победитель в номинации «Лучшее решение в области переноса персональных данных в РФ». Как и в прошлом году, приз получила компания IXcellerate. Если западная компания не хочет терять российский рынок, то выполняет требования регулятора и ищет ЦОД, где можно разместить свои системы хранения с персональными данными россиян. Такие компании прежде всего обращают внимание на имеющие хорошую международную репутацию дата-центры, предоставляющие услуги colocation на территории России. На подобных клиентов ориентирован ЦОД IXcellerate в Москве, который руководство компании рассматривает как ключевой в рамках системы ЦОДов стран БРИКС.

Семь лет прошло с момента появления идеи до ввода в эксплуатацию ЦОДа «Авантаж». Жюри оценило использованные при строительстве инновационные решения и присудило проекту победу в номинации «Лучшее решение в области инженерных систем». Более оперативной была компания «Фосагро», развернувшая на продукции Schneider Electric свой новый ЦОД в Череповце за четыре месяца (см. «ИКС» № 7–8'2017, с. 18). Жюри оценило скорость строительства и признало проект победителем в номинации «Лучшая интегрированная система (комплексное решение охлаждение + электроснабжение)». Сама компания Schneider Electric получила премию в номинации «Инновации в области снижения TCO ЦОДа».

Упорная борьба развернулась в номинации «Лучший проект облачного решения для ЦОДа». По критерию «надежность» предпочтительней выглядело конвергентное решение компании SoftLine «Единое облако федерального оператора на базе семи дата-центров», уже внедренное и успешно эксплуатируемое в семи центрах обработки данных страны. Но большинство судей проголосовало за новизну – первое в России гиперконвергентное облачное решение для среднего и крупного бизнеса, реализованное на базе платформы Cisco HyperFlex компанией Linxdatacenter.

В специальной номинации «За вклад в развитие профессионального сообщества» была отмечена C3 Solutions, активная молодая компания, постоянно оказывающая поддержку начинаниям, которые направлены на развитие рынка ЦОДов. «Наша концепция – meeting point для старых друзей. Мы каждое мероприятие стараемся сделать нестандартным», – пояснил получивший приз генеральный директор компании Максим Кыркунов.

■ ■ ■

...Прыгал шарик рулетки, крупье раздавал карты за столом для игры в покер, чудеса гравитации демонстрировал со стеклянным шаром фокусник-мим. Смогла расшевелить солидную публику на тацполе заводная кавер-группа «Русский бит». Но главное – было живое общение профессионалов в области дата-центров, новые знакомства, обсуждение новых идей и проектов. Праздник удался.

Николай Носов

Как важно быть «зеленым»

Запущенный в эксплуатацию в конце 2017 г. ЦОД Сбербанка России в «Сколково» стал победителем в номинации «Проект года» профессиональной премии Russian Data Center Awards. Динамические ИБП, прямой фрикулинг и сертификат LEED делают этот объект одним из самых «зеленых» в стране.

В декабре 2017 г. в инновационном центре «Сколково» состоялась церемония запуска нового мегаЦОДа Сбербанка, в которой приняли участие глава компании Герман Греф, вице-премьер Аркадий Дворкович, министр связи и массовых коммуникаций РФ Николай Никифоров и президент «Сколково» Виктор Вексельберг. Герман Греф нажал на установленном в ситуационном центре мегаЦОДа экране кнопку «Старт», заработал канал связи с дата-центром Сбербанка «Южный порт» и на панелях центра появились оперативные данные о работе информационных систем крупнейшего банка страны.

Запуск нового дата-центра значительно повышает надежность работы банка, обеспечивая «горячее» резервирование ИТ-систем на уровне ЦОДов, что важно в свете проведенной в Сбербанке централизации вычислительных систем. Резервирование ЦОДов позволит ему отказаться от арендуемых в настоящее время резервных площадок.

Конструкция ЦОДа

Здание мегаЦОДа «Сколково» состоит из четырех однотипных блоков (модулей). Ведется строительство пятого блока, и есть возможность дальнейшего пристраивания блоков к основному зданию.

В каждом блоке три этажа. Первый – энергетический. На нем расположены системы обеспечения электропитанием (энергетические системы построены по схеме 2N), дизельные динамические источники бесперебойного питания (ДИБП), логистические зоны и станции газового пожаротушения.

Заметим, что если в первом мегаЦОДе Сбербанка («Южный порт») были установлены статические ИБП, то для нового объекта были выбраны динамические системы. Такие технические решения все чаще применяют на мегаваттных объектах. Они более компактны по сравнению с классическими системами гарантированного и бесперебойного питания (ГБП), в которые, помимо статических ИБП, входят батареи аккумуляторов и внешние дизель-генераторные установки. ДИБП, по сути, представляет собой решение ГБП «все в одном»: для питания нагрузки в случае кратковременных отключений (как правило, до 10 с) служит раскрученный маховик, а для ее долговременной поддержки запускается установленный на одном валу с маховиком дизель-генератор.

В каждом блоке установлено шесть ДИБП – по три на основной и резервный каналы подвода электроэнергии. Мощность каждого ДИБП – 1800 кВт, суммарная мощность ДИБП в модуле – 11,28 МВт. Расходные баки ДИБП позволяют установкам проработать 2 ч, подземные топливные емкости обеспечивают полную автономность работы ЦОДа, суммарный объем запаса дизельного топлива на объекте – 200 т.

Для борьбы с возгораниями используется безвредное для здоровья людей огнетушащее вещество Novec 1230 («сухая вода»), которое является диэлектриком и не наносит вреда оборудованию. Системой автоматического газового пожаротушения оснащены все помещения с критической инфраструктурой: машинные залы, помещения распределительных устройств

Здание мегаЦОДа «Сколково» состоит из четырех однотипных блоков, продолжается строительство пятого блока

20 кВ, электрощитовые и серверные помещения систем диспетчеризации.

На втором этаже находятся машинные залы. В каждом блоке их четыре. Всего в 20 машинных залах планируется разместить 2 тыс. стоек, средняя расчетная нагрузка на стойку – 8 кВт. Все ИТ-оборудование имеет по два блока питания, каждый из которых подключен к своему лучу энергоснабжения (схема 2N). Вход в залы строго ограничен, на входе стоит кабина идентификации человека по лицу. Сейчас в ЦОДе работает только один машинный зал.

На третьем этаже размещаются системы охлаждения, использующие инновационные решения, которые руководитель проектов по строительству ЦОДов Сбербанка Сергей Шуршалин охарактеризовал как «фрикулинг с головой». В данном случае опять интересно сравнение схем охлаждения, выбранных для мегаЦОДов «Южный порт» и «Сколково». В первом дата-центре применена схема непрямого охлаждения внешним воздухом: наружный воздух поступает в теплообменники, где охлаждает воздух, циркулирующий во внутреннем контуре, который уже подается непосредственно к ИТ-оборудованию. Во втором ЦОДе реализована более энергоэффективная схема прямого фрикулинга.

В системе прямого фрикулинга наружный воздух, пройдя через систему фильтров, поступает в машинный зал. Для обеспечения требуемого уровня влажности задействуется система адиабатического увлажнения. Зимой к холодному наружному воздуху подмешивается теплый, подающийся из машинных залов. В жаркие летние дни для доохлаждения наружного воздуха в работу включается чиллерная система. К ИТ-оборудованию охлаждающий воздух с температурой 22°С поступает под фальшполом высотой 2 м. В машзалах используется схема разделения воздушных потоков с изоляцией горячих коридоров (температура отводимого от ИТ-оборудования воздуха – 37°С), через которые отработанный воздух выводится за пределы залов.

Для управления работой системы охлаждения специально создано программное обеспечение, по выражению С. Шуршалина – «практически искусственный интеллект», позволяющее анализировать метеосводку и заранее запасать холод при прогнозе резкого повышения температуры. Такой подход положительно скажется на энергоэффективности функционирования ЦОДа, расчетный коэффициент PUE которого составляет 1,3 (1,1 зимой и в пределах 1,4 летом).

Проект мегаЦОДа «Сколково» сертифицирован на соответствие стандартам Tier III Uptime Institute, причем, как считает С. Шуршалин, системы энергетики соответствуют требованиям Tier IV. Впоследствии будет проведена сертификация мегаЦОДа на соответствие стандартам Tier III по

Макет типового модуля мегаЦОДа: на первом этаже размещается энергетическое оборудование, на втором – серверные залы, на третьем – системы вентиляции и охлаждения

операционной устойчивости, как это уже сделано в дата-центре «Южный порт». Кроме того, мегаЦОД «Сколково» прошел экспертизу Руководства по энергоэффективному и экологическому проектированию (LEED-экспертизу) в США. Ему был присужден 51 балл, по завершении строительства здание получит сертификат соответствия экологическим стандартам LEED Silver.

Система автоматического газового пожаротушения

Мощность нового ЦОДа Сбербанка составит 30 МВт. Хранилища ЦОДа будут способны вместить до 1 эксабайта информации, что покроет потребности банка в хранении данных на 10 лет при сохранении текущих взрывных темпов роста их объема.

События и деньги

История постройки дата-центра началась еще в 2011 г., когда фонд «Сколково» зарезервировал на территории иннограда около 12 га земли под ЦОД и банковский технопарк. В 2014 г. был подписан договор аренды земельного участка с инвестиционными условиями. После того, как президенты Сбербанка и фонда «Сколково» согласовали основные параметры проекта, был разрабо-

В установленных в мегаЦОДе динамических ДИБП на одной оси совмещены маховик и дизель-генератор

тан комплект проектной документации и выдано разрешение на строительство.

Генеральным подрядчиком строительства дата-центра выступила входящая в группу ЛАНИТ компания «Инсистемс», с которой был заключен базовый контракт на 12,2 млрд руб. Сначала планировалось возведение четырех блоков (очередей) дата-центра, по четыре машинных зала в каждом. Впоследствии сумма контракта была увеличена в связи с решением о создании пятого блока.

В итоге расходы на строительство и инженерные системы, по словам Г. Грефа, составили примерно 14 млрд руб. Ожидаемый срок окупаемости ЦОДа – два года. «Мы закончили строительство четырех очередей. Сейчас строится пятая очередь, и нужно принять решение о строительстве шестой, – сказал глава крупнейшего российского банка и добавил: – Пока нам достаточно четырех очередей, пятую очередь мы рассматриваем как потребность нашей экосистемы, а шестая – это перспектива».

Выделяемое в машинных залах тепло используется для отопления. По оценкам Сбербанка, в перспективе это позволит уменьшить расходы на обогрев здания примерно на 5 млн руб. в год. Кроме того, согласно предварительным расчетам, система поможет в будущем экономить до 100 млн руб. в год на электроэнергии по сравнению со стандартной системой с прецизионными кондиционерами.

Вентиляционные установки системы прямого фрикулинга

«Мы постарались применить все самые современные технологии, которые были доступны. Также перед нами ставилась задача максимально использовать российские разработки», – заявил Г. Греф.

По словам С. Шуршалина, в ЦОДе работают отечественные системы хранения данных «Баум». «То, что можно было использовать российское, все использовали. Некоторые системы были специально созданы для этого ЦОДа – экологичные системы энергетического обеспечения, охлаждения, отопления», – пояснил А. Дворкович.

Представители Сбербанка утверждают, что ЦОД «Сколково» станет самым большим и самым инновационным центром обработки данных в России и одним из крупнейших дата-центров подобного класса в Европе.

Николай Носов

Центр управления мегаЦОДом «Сколково»

Закон о безопасности КИИ и аутсорсинг: вопросов еще много

Утверждены правила категорирования объектов критической информационной инфраструктуры.

Вступивший в январе в силу закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ вызвал много вопросов. Полное понимание у регулятора и объектов регулирования появится, когда будут выпущены все нормативные правовые акты, но начинать работы по реализации закона надо уже сейчас. Прежде всего нужно понять, к каким категориям критической информационной инфраструктуры (КИИ) относятся имеющиеся в организации информационные системы.

Категории значимости КИИ

Картину частично проясняет подписанное 8 февраля 2018 г. Постановление Правительства РФ № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации...». Согласно этому постановлению, вводятся три категории (наивысшая – первая) значимости объектов КИИ. Так, если нарушение функционирования сети связи затронет не всю территорию муниципального образования и без связи останутся менее 50 тыс. человек, то по этому показателю объект КИИ не относится к значимым, если же будет затронута вся территория (или если без связи останутся от 50 тыс. до миллиона человек), то объект относится к третьей категории. Если территория, на которой возможно прекращение или нарушение функционирования сети связи, выходит за границы субъекта Федерации (или без связи останутся более 5 млн человек), то объект – первой категории значимости.

Как напомнила на 23-м международном форуме «Технологии безопасности» заместитель начальника управления ФСТЭК России Елена Торбенко, в ФЗ-187 выделены 12 областей деятельности, в которых функционируют объекты КИИ:

- здравоохранение;
- наука;
- транспорт;
- связь;
- банковская сфера и иные сферы финансового рынка;
- топливно-энергетический комплекс;
- атомная энергетика;
- оборонная промышленность;
- ракетно-космическая промышленность;
- горнодобывающая промышленность;
- металлургическая промышленность;
- химическая промышленность.

Законодательство довольно либерально в плане категорирования объектов КИИ. Субъекты хозяйственной деятельности: государственные органы и учреждения, российские юридические лица и индивидуальные предприниматели – проводят его сами. Чтобы понять, является ли организация субъектом КИИ, нужно посмотреть уставные документы, лицензии и другие разрешительные документы на виды деятельности, свериться с общероссийским классификатором видов экономической деятельности.

МНЕНИЕ ЭКСПЕРТА

Безопасность КИИ: взгляд облачного провайдера

Центр финансовых технологий предлагает банкам услуги аутсорсинга ИТ-инфраструктуры и переноса банковских бизнес-процессов на инфраструктуру ЦОДов компании. Мы планируем определять категории значимости КИИ наших существующих клиентов и выполнять все требования регуляторов по обеспечению безопасности облачных сервисов, предоставляемых банкам по модели SaaS.

В действующих договорах уже прописана необходимость выполнения сторонами действующего законодательства, так что заключать дополнительные соглашения с банками, скорее всего, не придется. Если банки выступят с предложениями о дополнительных мерах выполнения положений нового законодательства, мы, безусловно, будем над этим работать. Но в этом нет ничего принципиально нового – мы постоянно обсуждаем с банками возможности внедрения нового функционала в сфере инфобезопасности.

По договору мы имеем обязательства по обеспечению работоспособности инфраструктуры на нашей стороне. При прекращении работы КИИ регулятор обратится в банк, но банк сможет транслировать свои риски на нас – как и в случае соблюдения закона о защите персональных данных. Конечно, закон новый, но скорее всего, трактоваться он будет именно так: каждый отвечает за свою часть КИИ.

Закон № 187-ФЗ будет стимулировать банки к использованию облачных аутсорсинговых моделей, что позволит с минимальными затратами выполнить требования нового законодательства.

Алексей Леонов, директор дирекции информационной безопасности, Центр финансовых технологий

Основные этапы категорирования объектов КИИ РФ	Результат
Создание комиссии по категорированию	Приказ о создании комиссии
Анализ исходных данных для категорирования	Перечень объектов КИИ, подлежащих категорированию. Направляется в ФСТЭК в течение пяти дней после создания перечня
Категорирование объектов КИИ	Акт категорирования объекта КИИ
Направление сведений о категорировании в ФСТЭК РФ (в течение 10 дней после выпуска акта категорирования)	Внесение в реестр значимых объектов КИИ

По материалам доклада зам. начальника управления ФСТЭК России Е. Торбенко на ТБ-Форуме

▲ **Порядок действий при категорировании объектов КИИ РФ**

Что делать?

Организация – субъект КИИ в первую очередь должна составить перечень объектов КИИ, подлежащих категорированию. В принципе надо дождаться письменных разъяснений от регулятора, но лучше сразу выпустить приказ о создании комиссии по категорированию и назначить ответственных за планирование мероприятий.

Комиссия проанализирует исходные данные и сформирует перечень объектов КИИ, подлежащих категорированию. Далее в течение пяти дней перечень в установленной форме должен быть отправлен в ФСТЭК. На устранение замечаний регулятора и категорирование объектов КИИ отводится год со дня утверждения субъектом КИИ перечня объектов. Это крайний срок для составления акта категорирования объектов КИИ и направления (в течение 10 дней после утверждения) в ФСТЭК сведений о результатах категорирования.

Категорирование объектов КИИ проводится с учетом их политической, экономической, социальной, экологической значимости и важности для обеспечения обороны страны. Оценка проводится по каждому критерию, а категория присваивается по высшему значению.

ФСТЭК проверяет правильность категорирования, при необходимости отправляет материалы субъекту КИИ на доработку и вносит данные в реестр значимых объектов КИИ. Пересмотр категории значимости производится не реже, чем раз в пять лет.

Вопросы аутсорсинга КИИ

Может возникнуть ситуация, когда объект КИИ принадлежит одному субъекту, но в целях хозяйственной деятельности используется другим субъектом. «В этом случае категорирование производит субъект – владелец КИИ на основании данных, которые он получает от хозяйствующего субъекта», – пояснила Е. Торбенко.

В теории это понятно, но вот на практике реализовать не всегда просто. Возьмем облачного провайдера, который оказывает услуги бухгалтериям по модели SaaS, например предоставляет «1С». Получается, что он должен послать всем своим клиентам запрос, не является ли работа их бухгалтерии критической для политической, экономической или социальной ситуации в регионе и стране? Иначе как он сможет категорировать свою информационную инфраструктуру?

А если услуга предоставляется по модели IaaS? Всегда ли провайдеры знают, для каких задач используется выделяемая клиенту инфраструктура? Была ли проведена на нее атака, о которой он теперь обязан сообщить регулятору? Причем об-

МНЕНИЕ ЭКСПЕРТА

Облачные провайдеры как субъекты КИИ

Алексей Лукацкий, бизнес-консультант по безопасности, Cisco

Сегодня многие организации с целью сфокусироваться на своем основном бизнесе передают часть своей инфраструктуры или данных внешним провайдерам. А те, в свою очередь, должны соблюдать требования действующего законодательства. Однако в ситуации с законом ФЗ-187 не всегда понятно, кто подпадает под определение субъекта КИИ. Попробуем разобраться с этим применительно к облачным провайдерам.

Самый простой случай, когда облачный провайдер является оператором связи. Тогда он по определению из ФЗ-187 становится субъектом КИИ и на него распространяются все или часть требований закона (в зависимости от наличия значимых объектов). Но что делать облачному провайдеру, не имеющему лицензии в области связи, но которому, допустим, банк – субъект КИИ доверил обработку своих данных?

На мой взгляд, надо внимательно рассмотреть определение субъекта КИИ. В примере с банком это юрлицо, которому на праве собственности, аренды или на ином законном основании принадлежит информационная система, функционирующая в банковской сфере. Принадлежит ли банку облачная ИС на праве аренды? В зависимости от модели аутсорсинга (IaaS, PaaS или SaaS) – да. А есть ли у облачного провайдера ИС, функционирующая в банковской сфере? Тут надо смотреть более внимательно. В случае с моделями IaaS и PaaS я думаю, что нет. В случае же с SaaS надо изучать функционал конкретной системы.

Если облачный провайдер не является субъектом КИИ, означает ли это, что он не должен выполнять требования к субъектам КИИ? Вопрос правильный. Если банк передает часть своих данных в облако, то это не снимает с него обязанность обеспечить защиту данных по требованиям положения Банка России № 382-П, приказа ФСТЭК № 21 или закона ФЗ-187. Это обязанность, от которой нельзя отказаться и которую нельзя ни на кого переложить, – ответственность

лачный провайдер может не быть владельцем инфраструктуры, а тоже брать ее в аренду. Тогда ответственность перекладывается на владельцев дата-центра. Еще сложнее ситуация с предоставлением услуги по модели colocation. На арендуемых вычислительных мощностях клиент может развертывать все что угодно, контролировать это провайдер не состоянии.

И всегда ли поставщик услуг получит ответ на свой запрос о категории значимости развернутой у него информационной системы? Не помогут и общие данные о деятельности заказчика. Компания, занимающаяся водоснабжением, формально не относится к тем сферам деятельности, где функционируют объекты КИИ. Но может оказаться, что она поставляет воду для АЭС и используемая ею информационная инфраструктура относится к первой категории значимости.

Крайним в такой ситуации окажется дата-центр. Ответственность не малая – при наступлении тяжелых последствий из-за неправомерных воздействий на КИИ с 1 января текущего года можно получить по ст. 274.1 УК РФ до 10 лет лишения свободы. Хотя в данном случае скорее грозят шесть лет за нарушение правил эксплуатации средств хранения, обработки или передачи содержащейся в КИИ информации.

Однако категорирование – это только первый этап. Дальше начнется самое сложное – обеспечение безопасности КИИ. Причем чем выше значимость КИИ, тем требования жестче. И тут появляются новые возможности для аутсорсинга. Прежде всего аутсорсинга информационной безопасности, ведь большинству предприятий будет не по карману содержать специалистов по ИБ, не говоря уже про собственный ситуационный центр ИБ (SOC). Да и перекладывание ответственности на владельцев информационных инфраструктур будет способствовать росту использования облачных моделей. У дата-центра есть экспертиза, специалисты, программные и аппаратные средства обеспечения информационной безопасности. Провайдерам информационных инфраструктур легче выполнить требования регуляторов.

Вопросов много, но они решаемые. Главное – активно их задавать, ведь ФСТЭК не может продумать все сам за все хозяйствующие субъекты страны. Посылать вопросы можно на электронную почту ФСТЭК otd22@fstec.ru с пометкой «Вопросы по КИИ». В конце концов, в этом заинтересованы все.

Николай Носов

Исходные данные для категорирования объектов КИИ РФ

- Сведения об объекте КИИ.
- Процессы (управленческие, технологические, производственные, финансово-экономические) в рамках выполнения функций субъекта КИИ.
- Состав информации, обрабатываемой объектами КИИ, сервисы, предоставляемые объектами КИИ.
- Декларация промышленной безопасности опасного производственного объекта, декларация безопасности гидротехнического сооружения, паспорт объекта ТЭК, на которых функционирует объект КИИ, если их разработка предусмотрена законодательством РФ.
- Сведения о взаимодействии объекта КИИ с другими объектами КИИ.
- Угрозы безопасности, а также данные о компьютерных инцидентах, произошедших на объектах КИИ данного типа.

По материалам доклада зам. начальника управления ФСТЭК России Е. Торбенко на ТБ-Форуме

МНЕНИЕ ЭКСПЕРТА

за нарушение все равно ляжет на банк. Вспомните ФЗ-152. Вы могли привлечь сколь угодно много обработчиков персональных данных, но ответственность за их утечку лежала все равно на вас, а не на них. То есть субсидиарная ответственность в данном случае отсутствует, и привлечь обработчика персональных данных к ответственности можно только, если в договоре с ним зафиксированы требования, нарушение которых и привело к утечке, и данный факт был доказан.

Аналогичная ситуация с ФЗ-187. Субъект КИИ для облегчения своей жизни может привлекать кого угодно, но ответственность за нарушение закона все равно лежит на нем. Чтобы соблюсти все требования закона, банк должен предъявить соответствующие требования из подзаконных актов ФСТЭК (если у него есть значимые объекты) облачному провайдеру в рамках договора (если провайдер согласится). И тогда облачный провайдер должен будет соблюдать все требования ФСТЭК, но не потому, что он субъект КИИ, а потому, что так записано в договоре между ним и банком. В договоре с провайдером должны быть перечислены защитные меры и приведен план проверок выполнения мер, что является обычной практикой при аутсорсинге.

С другой стороны, как правильно отметила Елена Торбенко на ТБ-Форуме-2018, при определении того, является ли организация субъектом КИИ, надо руководствоваться различными классификаторами деятельности. Одним из них является ОКВЭД 2, в котором есть класс 63.11 «Деятельность по обработке данных, предоставление услуг по размещению информации и связанная с этим деятельность». Этот класс ОКВЭД относится к разделу «Деятельность в области информации и связи». Получается, что облачный провайдер сам по себе является субъектом КИИ, работающим в сфере информации и связи, невзирая на то, кто с ним заключает договор и какие услуги он оказывает по договору. Для меня это неожиданный поворот, который показывает, что процедура категорирования не так проста, как казалось сначала. Тут, конечно, можно сказать, что в ФЗ-187 речь идет только о сфере связи, а облачный провайдер – это, в первую очередь, сфера информации. Но это уже совсем иная дискуссия, более сложная и долгая. Попробовать пойти по этому пути можно, но с непредсказуемыми последствиями.

Цифровая трансформация: государственные цели и облачные инструменты

Понимание, что российской экономике нужна цифровая трансформация – глубинные преобразования производственных и бизнес-процессов, а также схем взаимодействия участников экономической деятельности, – уже существует на самом высоком уровне.

Как, с помощью каких технологий и кем эти преобразования должны проводиться? Ответ на этот вопрос сообща искали участники 7-й международной конференции Cloud & Digital Transformation, организованной «ИКС-Медиа» и собравшей в этом году около 300 делегатов.

Сценарии цифровизации

Процесс преобразований, основанных на применении высоких технологий, был актуализирован летом-осенью 2017 г., когда правительство нашей страны утвердило государственную программу «Цифровая экономика Российской Федерации». Госпрограмма трактует цифровую экономику как хозяйственную деятельность, в которой ключевую роль играют данные в цифровой форме и которая способствует формированию единого информационного пространства, развитию информационной инфраструктуры в стране, созданию и применению российских ИКТ, а также формированию новой технологической основы для социально-экономической сферы. Документом определены индикаторы, которые должны свидетельствовать о том, что цели программы достигнуты. Так, согласно госпрограмме, в 2024 г. в России будут функционировать не менее 10 компаний-лидеров (операторов экосистем), конкурентоспособных на глобальных рынках. Кроме того, к этому сроку в стране заработают 10 цифровых интеллектуальных платформ для здравоохранения, образования, ЖКХ.

Процесс формирования единой информационной среды посредством интеграции электронных сервисов, продуктов и информационных систем – такое определение дала цифровой трансформации Татьяна Толмачева, управляющий партнер аналитического агентства iKS-Consulting. В качестве интеллектуального вклада агентства в изучение этого процесса она предложила считать электронные сервисы «единицей измерения» уровня цифровизации экономики.

Таких сервисов в России уже создано и используется немало. Официальная статистика портала госуслуг показывает, что электронное взаимодействие по линии «государство – бизнес – граждане» находится далеко не на начальном уровне. По данным Минкомсвязи России, в 2017 г. услугами этого интернет-ресурса федерального значения воспользовались 62 млн россиян, т.е. практически все экономически активное население страны; сертификаты электронной цифровой подписи получили 15,2 млн юридических и физических лиц; необходимые для участия в торгах сертификаты усиленной ЭЦП – 2,5 млн. Государство сегодня активно занимается и внутренней автоматизацией бизнес-процессов бюджетирования, управления госзакупками, управления комплексом регионального и муниципального имущества, мониторинга исполнения государственных программ и территориального планирования. И важно, по мнению аналитика, что оно системно подходит к построению инфраструктуры цифровой экономики, включающей в себя такие «узлы», как межведомственные государ-

CLOUD & DIGITAL
TRANSFORMATION

ственные распределенные сети и электронный документооборот, единая система аутентификации и идентификации, платформы анализа больших данных, а также системы шифрования и информационной безопасности.

Для Министерства энергетики РФ сценарий цифровой трансформации предусматривает формирование единой доверенной информационной среды для обмена технологическими данными как между субъектами отрасли электроэнергетики, так и с компаниями из смежных отраслей, внедрение риск-ориентированного управления, создание системы мониторинга надежности энергоснабжения и управления ею. Также ведомство планирует разработать систему формирования отраслевых заказов для стимулирования машиностроительной и микроэлектронной промышленности, а на завершающем этапе оно будет готово предоставлять сервисы конечным потребителям. По словам Елены Медведевой, заместителя директора департамента оперативного контроля и управления в электроэнергетике Минэнерго России, по результатам НИР и пилотных проектов ведомство в этом году представит типовые технические требования к платформе единой доверенной цифровой среды, необходимые для проведения конкурса. В числе возможных его участников рассматриваются «Ростелеком», «Ростех» и дочерняя компания «Росатома» – РАСУ.

В настоящее время Минэнерго проводит два пилотных проекта с компанией «Ростелеком», занимающейся оказанием услуг для нужд госсектора. Ее Единый центр компетенций «Ростелеком – Центры обработки данных» (РТК-ЦОД) представляет собой группу из шести компаний, под управлением которых в России работают в общей сложности 5268 стоек с оборудованием в дата-центрах суммарной площадью 46 тыс. кв. м. На базе объединенных волоконно-оптической магистральной сетью дата-центров РТК-ЦОД предоставляет органам государственной власти из своего распределенного облака такие сервисы, как виртуальные рабочие места, инфраструктура как сервис (IaaS) и платформа как сервис (PaaS), а также платформы управления облачной инфраструктурой, оборудование в аренду и техническую поддержку.

Будущее за облаками

Если взглянуть на российский рынок облачных сервисов в целом, то можно увидеть, что на протяжении 2016–2017 гг. он рос в среднем на 27% в год. По предварительным оценкам iKS-Consulting, его объем по итогам прошлого года – 49,3 млрд руб. Сегмент IaaS этого рынка достиг зрелости, использование инфраструктуры как

сервиса стало стандартным для крупных российских компаний, которые в совокупности с компаниями среднего размера обеспечивают более 80% всей его выручки.

В ближайшем будущем на рынок облачных сервисов, по мнению Станислава Мирина, консультанта iKS-Consulting, могут серьезно повлиять два тренда. Первый – это выход на рынок операторов связи, заинтересованных в том, чтобы компенсировать снижение доходов от телеком-услуг развитием ИТ-направления своего бизнеса. Второй – активизация провайдеров с Востока, приходящих на смену западным игрокам, чья доля сокращается в связи с введением так называемого налога на Google.

В ближайшее время на строчки в рейтинге «Топ-10 игроков на рынке IaaS» способны претендовать такие компании, как CITIC Telecom CPC и Huawei. Первая, дочерняя структура одной из крупнейших инвестиционных корпораций Китая CITIC Group, вышла на российский рынок в 2017 г. путем приобретения телекоммуникационного сегмента ГК Linx. Сегодня она продвигает в России решения на базе технологии программно определяемой распределенной сети WAN, SD-WAN, позволяющие предприятиям в автоматическом режиме, используя любое интернет-подключение, быстро и экономично развернуть и настроить связь между центральным офисом и его филиалами, в том числе в разных регионах страны и даже мира.

Компания Huawei в марте запустила в России публичное облако в партнерстве с 3data, российским оператором сети премиальных ЦОДов. Цель партнеров – построить насыщенное сервисами облако. На момент запуска Huawei 3data Cloud потенциальным клиентам было доступно 20 сервисов, и, по словам Павла Вишнякова, директора по работе с партнерами компании Huawei, до конца 2018 г. их количество планируется утроить. Все сервисы ориентированы на предприятия, переживающие процесс цифровой трансформации бизнеса, независимо от его масштаба.

К 2020 г. в мире как минимум 50% ИТ-бюджетов будет направляться на использование облачных сервисов и инфраструктур. Такой прогноз сделал Константин Юров, руководитель технической экспертизы гибридных облачных решений IBM. Уже сегодня большинство компаний задействуют несколько облаков: из одних они получают приложения как сервис, в другие выносят свою ИТ-инфраструктуру и т.д. В перспективе использование мультиоблачных сред будет нарастать. Компания IBM видит свою задачу в том, чтобы помочь предприятиям бесшовно интегрировать разные типы облаков в единую инфраструктуру. Ее стремление поделиться экспертизой в области цифровой трансформации и предоставить возможность из облака пользоваться уникальными сервисами разделяют другие глобальные вендоры.

Являясь удобным инструментом для трансформации процессов разработки, предоставления и потребления ИТ-сервисов, облачная модель очень подходит для реализации технологического базиса цифровой экономики. Подводя черту, хочется отметить, что курс на перевод российской экономики на цифровые «рельсы», зафиксированный в госпрограмме «Цифровая экономика», открывает перед всеми участниками рынка ИКТ новые возможности, которыми можно и нужно воспользоваться.

Александра Крылова

Китайские облака пришли в Россию

Huawei создает новое направление в структуре российского бизнеса – Huawei Cloud и запускает у нас в стране первое за пределами Китая публичное облако, работающее под брендом компании.

В рамках Huawei 3data Cloud в России доступно более 20 публичных облачных сервисов, позволяющих заказчику построить полноценную облачную инфраструктуру с управлением через онлайновый кабинет самообслуживания или посредством задокументированных API. Количество сервисов все время увеличивается и достигнет 50 к концу 2018 г. При появлении спроса компания может локализовать любой нужный сервис из своей глобальной экосистемы, в которой имеются сервисы для сферы электронной коммерции, ритейла, финансов, логистики и здравоохранения. Есть специализированные решения в области высокопроизводительных вычислений, интернета вещей и разработки мобильных приложений.

«Мы делаем бизнес на предоставлении технологий, а не данных. Это принципиальное отличие Huawei от других облачных провайдеров, выросших из интернет-компаний», – пояснил Ван Вэй, директор направления Huawei Cloud в России.

Российским партнером Huawei выступает компания 3data, которая предоставляет свои ЦОДы, расположенные в районах бизнес-активности столицы. В настоящее время облако Huawei 3data Cloud развернуто в ЦОДе 3data на Новорязанской улице, в июне планируется подключить второй ЦОД и развернуть систему самообслуживания. Компания 3data станет заниматься эксплуатацией облака, первой и второй линией поддержки клиентов. За третью линию поддержки будет отвечать сама Huawei. Каналы связи поддерживает компания «Мастертел», которой принадлежит более 7000 км оптики в Москве и области.

Ван Вэй: «В эпоху цифровой экономики индикатором прогресса является проникновение облачных услуг»

По оценкам Huawei, рост российского облачного рынка за последний год составил около 25%, в то время как рынок классической ИТ-инфраструктуры вырос всего на несколько процентов. Развертывание облака Huawei в России свидетельствует об оптимизме, с которым компания оценивает дальнейшее развитие облачных технологий в нашей стране.

Учение без отрыва от лечения

Проект «УчимЗнаем» теперь представлен в восьми регионах России – новый класс открылся в Областной детской клинической больнице в Ростове-на-Дону. В классе будут учиться дети, находящиеся на длительном стационарном лечении в отделении детской онкологии и гематологии с химиотерапией.

Новые знания и общение заряжают оптимизмом и помогают детям настроиться на выздоровление

Цель проекта «УчимЗнаем» – создать единое социально-образовательное пространство для детей, которые вынуждены подолгу находиться в больницах. Компания Samsung, технический партнер проекта, предоставляет необходимое для образовательных целей оборудование. Так, класс проекта в Ростове-на-Дону оснащен современной компьютерной техникой, в том числе сенсорной телевизионной панелью, компьютером и планшетами для всех учеников. Дети смогут не только получать новые знания и общаться со сверстниками на уроках, но и сдавать экзамены и участвовать в олимпиадах. Преподавать в классе будут специально подготовленные тьюторы – учителя ростовского лицея № 11.

Проект «УчимЗнаем» начал реализовываться в 2014 г. ГБОУ г. Москвы «Школа № 109» («Школа Ямбурга») при поддержке Министерства образования и науки РФ, а также региональных ведомств. География проекта постоянно расширяется: с 2016 г. его участниками стали детские медицинские учреждения в Московской и Ленинградской областях, Хабаровском крае, Орловской области, Ростове-на-Дону, Калининграде, Красноярске и Воронеже. В апреле 2018 г. новый класс в рамках проекта планируется открыть в Центре онкогематологии при Пермской краевой детской клинической больнице.

«Все в одном» для резервного копирования

Компания Commvault представила в России интегрированный программно-аппаратный комплекс HyperScale Appliance, в котором совмещены функции хранения и защиты данных.

Задача резервного копирования данных и управления ими критична для любой современной компании или ор-

А. Вышлов: «В России немало заказчиков, для которых проект без "железа" – это не проект. Теперь мы становимся им интересными»

ганизации, для которых информация – важнейший бизнес-актив. Компания Commvault решила пойти по пути объединения функций, которые в традиционной архитектуре защиты данных выполняются отдельными серверами, в единый программно определяемый стек.

Решение, получившее название HyperScale, предлагается в двух вариантах: в виде ПО и готового программно-аппаратного комплекса. Такой комплекс HyperScale Appliance рассчитан на емкость от 32 до 80 Тбайт.

«Появление в нашем продуктовом портфеле готового программно-аппаратного комплекса даст нам возможность попасть в сегменты, где мы ранее не присутствовали», – считает Андрей Вышлов, руководитель офиса Commvault в России и СНГ.

Чисто программное решение HyperScale не имеет ограничений по емкости. В принципе это ПО может работать практически на любых серверах x86. Но чтобы гарантировать такую работу, специалисты Commvault разработали эталонную архитектуру и протестировали решения ряда производителей на соответствие ее требованиям. Эту процедуру прошли серверы Dell EMC, Fujitsu, Huawei, HPE, Lenovo, SuperMicro и др. Однако, как отмечают в Commvault, наиболее тесное сотрудничество ведется с Cisco. Совместное с этим вендором решение – ScaleProtect представляет собой ПО HyperScale, развернутое на платформе Cisco UCS.

ПО HyperScale реализует такие функции управления данными, как дедупликация, непрерывный мониторинг, управление изменениями, защита и аварийное восстановление. Кроме того, поддерживаются возможности интеграции с сервисами публичных облаков, например AWS, Google, Oracle, Azure и др. Наличие этих возможностей в HyperScale позволяет реализовывать эффективные гибридные и мультиоблачные схемы, к которым все чаще прибегают заказчики.

Extreme Networks: от A до Z

Совершив ряд знаковых приобретений, Extreme Networks за последние пять лет из игрока «второго десятка» поднялась до уровня номер три среди производителей сетевых решений.

Недавние события – покупка Wi-Fi-подразделения компании Zebra Technologies, сетевого бизнеса Avaya и занимающегося решениями для ЦОДов «куска» Brocade – превратили Extreme Networks в компанию с оборотом $1,2 млрд. В России в прошлом году ее оборот увеличился на 170%, а главные направления роста связаны с проектами в ЦОДах, в ритейле, а также с оборудованием нескольких стадионов для Чемпионата мира по футболу.

Представляя стратегию развития, Кирилл Жуков, технический директор Extreme Networks в Северной и Восточной Европе, подчеркнул, что в ее основе – сохранение интересов заказчиков. Укрупнившаяся компания сохранит все сервисные обязательства купленных производителей, а на транзитный период – и их существующие каналы продаж. Более того, в Extreme Networks не намерены отказываться ни от одного из продуктов приобретенных компаний, хотя со временем они будут интегрированы в единую продуктовую линейку.

Благодаря разработкам Avaya и Brocade компания Extreme Networks теперь превратилась, пожалуй, в «королеву» сетевых фабрик. Фабрики Brocade составляют основу предложения Extreme для дата-центров – Agile Data Center. А разработанная для кампусных сетей Avaya Fabric Connect стала основой решений Automated Campus. В свое время большинство сетевых производителей сосредоточились на фабриках для ЦОДов, а Avaya, чуть ли не единственная, акцентировала усилия на разработке «кампусной» фабрики.

К. Жуков: «Ориентировочно через полтора-два года все продукты приобретенных компаний будут интегрированы в единую линейку»

Что касается развития решений Wi-Fi, то на 2018 г. намечен выпуск точек доступа с поддержкой нового стандарта 802.11ax. В новых ТД при их загрузке будет предоставлена возможность выбора ОС: ExtremeWireless (так называются собственные решения Wi-Fi Extreme) или WiNG (решения бывшей Zebra). Это первый шаг по интеграции двух линеек Wi-Fi-продукции. Следующий шаг – выпуск универсального контроллера, который будет способен работать с точками доступа обоих семейств. Ну а затем – переход на единую линейку продуктов.

ИБП General Electric начали собирать в России

В подмосковном Долгопрудном состоялось официальное открытие площадки по производству промышленных ИБП под торговой маркой «Абитех».

Евгений Михеев («Абитех»): «Собранные изделия тестируются поблочно. После сборки блоков в систему бесперебойного питания производится тестирование комплекса в целом»

Весной прошлого года компания «Абитех» подписала лицензионное соглашение с GE Industrial Solutions о праве проведения сборки, тестирования и продажи оборудования на территории России. В течение года было выбрано соответствующее требованиям GE здание, создана производственная компания «Абитех-ПРО» и развернута производственная площадка, включающая цех сборки ИБП и помещение для их тестирования. В январе были собраны первые ИБП, полностью соответствующие стандартам GE.

После механической сборки устройства тестируются сначала вручную, а затем в автоматическом режиме, по программам GE. В ходе тестирования проверяется, как ИБП работают при различных нагрузках, возможен ли пробой изоляции, насколько правильно функционируют узлы при коротком замыкании. Протоколы испытаний передаются покупателю оборудования.

Первая линейка устройств бесперебойного питания бренда «Абитех» (это название сменило первоначально планировавшееся «А-ИСТ») будет поддерживать диапазон мощностей от 10 до 160 кВА.

«Абитех-ПРО» планирует производить пять серий однофазных и трехфазных ИБП в диапазоне номинальной мощности 3–600 кВА, отличающихся числом фаз на входе/выходе, возможностью объединения нескольких ИБП в параллельную группу, наличием встроенного сервисного байпаса, применением трансформаторной технологии.

Первые заказчики – проводящие импортозамещение государственные организации. Уже сейчас локализованы процессы сборки и тестирования ИБП, разработана конструкторская документация на российские изделия. В дальнейшем планируется постепенная локализация узлов.

Дома абонентов «Триколор ТВ» смогут «поумнеть»

Развивая свою стратегию – ориентироваться на предоставление сервисов Digital lifestyle, оператор «Триколор ТВ» объявил о запланированном на август 2018 г. запуске под собственным брендом услуги «Умный дом».

Фокусироваться на развертывании новых цифровых сервисов, выходящих за рамки телевизионных услуг, активизировать работу в B2B-сегменте, предоставлять частным и корпоративным клиентам спутниковый интернет, а также возможности нелинейного, персонализированного потребления контента компанию подталкивают отток телеаудитории в Сеть, переход на нелинейное смотрение, невысокая цена мобильного доступа в интернет. «Рынок уже насыщен», – констатирует генеральный директор «Триколор ТВ» Алексей Холодов. Правда, оператору и в этих условиях удается расти – его выручка в 2017 г. увеличилась на 6,7%, до 19,1 млрд руб., абонентская база достигла 12,28 млн домохозяйств (+140 тыс.).

Один из шагов по развитию сервисов был сделан в 2016 г., когда в партнерстве с Eutelsat Networks была запущена услуга спутникового интернета (в прошлом году ее подключили 3 тыс. абонентов, доля «Триколор ТВ» на рынке спутникового интернета в 2017 г. составила 7%).

Следующий шаг на этом пути – «Умный дом». В компании видят серьезный спрос на такую услугу, но не столько в западном ее понимании, когда за счет автоматизации управления энергопотреблением и отоплением клиенты экономят на оплате услуг ЖКХ, сколько с точки зрения обеспечения безопасности дома (своевременное информирование о возгораниях, проникновении посторонних, утечках газа и т.п.). В основе решения – абонентский приемник, к которому подключается шлюз. В доме устанавливаются различные датчики – открытия/закрытия дверей и окон, движения, протечек, задымления, температуры, влажности и т.п., а также «умные» выключатели, розетки и лампы. Управлять «умным» домом можно будет через экранное меню телевизора с помощью пульта ДУ, а также удаленно через специальное приложение с мобильных устройств. Клиентам предложат такие функции, как мониторинг, видеонаблюдение, уведомление и удаленное управление.

А. Холодов: «Мы стремимся перестать быть исключительно оператором платного ТВ и намерены дальше двигаться в направлении Digital lifestyle»

30 мая в Москве (Metropol Hotel Moscow) состоится 2-я конференция Forbes **«Как увеличить прибыль компании с помощью Big Data»**.

Термин Big Data существует более 10 лет. Но всего 15% компаний умеют работать с большими данными и эффективно использовать их для получения финансовой выгоды.

Есть две основные причины: компании либо не знают, как получить данные для анализа в своем бизнесе, либо не умеют извлекать пользу из собираемого объема данных. На конференции эксперты Forbes расскажут, как решить обе задачи.

В рамках конференции состоится круглый стол «Инвестиционные возможности» с участием инвесторов. У участников конференции будет возможность представить свои проекты инвесторам, а у инвесторов – сформулировать свой интерес.

Организатор: Forbes.

www.forbes.ru/konferencii/bigdata

выставки, семинары, конференции

Дата и место проведения, организатор, сайт	Наименование мероприятия
18.04. Москва ИКС-МЕДИА http://clubdc.ru	**Data Center Club**
18.04. Москва РАЭК https://2018.rif.ru	Российский интернет-форум (РИФ + КИБ 2018)
23–24.04. Москва Infor-media Russia www.infosecurity-forum.ru	XI межотраслевой форум «CISO FORUM 2020: взгляд в будущее»
24.04. Москва «ТелеСпутник» http://telemultimedia.ru	TeleMultimedia Forum 2018
26.04. Москва ИКС-МЕДИА www.dcdeforum.ru	**6-я ежегодная конференция и выставка Data Center Design & Engineering**
15–16.05. Москва Positive Technologies www.phdays.com/ru	Международный форум по практической безопасности Positive Hack Days 8: Digital Bet
23–24.05. Москва Oborot http://expo.oborot.ru	Выставка технологий для интернет-торговли ECOM Expo'18
24–25.05. Москва РАЭК http://2018.sp-ic.ru	Санкт-Петербургская интернет-конференция СПИК 2018
31.05. Алматы ИКС-МЕДИА http://dcforum.kz	**3-я международная конференция и выставка «ЦОД 2018: модели, сервисы, инфраструктура»**

Присылайте анонсы ваших мероприятий на IKSMEDIA.RU

Еще больше на

18–20 апреля в Подмосковье состоится **22-й Российский интернет-форум** (РИФ + КИБ 2018).

РИФ + КИБ 2018 проходит в формате трехдневного выездного мероприятия, состоящего из многопотоковой конференции, «народной» Программы 2.0, масштабной выставки и внепрограммных мероприятий от оргкомитета и партнеров РИФа.

В эксклюзивных докладах спикеры из самых разных отраслей расскажут о будущем интернета, технологий, коммуникаций, бизнеса, цифровой экономики и влиянии «цифры» на «офлайн».

РИФ. PaperLess предлагает испытать новые возможности чипированных бейджей участников – они будут работать по технологии PaperLess by RUVENTS в специальных интерактивных зонах и на выставке.

Стартапы, молодые предприниматели и инвесторы получат собственный «кусочек РИФа» в формате популярного проекта UpStart, который объединит в себе специальные секции в программе, место на выставке и внепрограммные мероприятия, полезные и интересные для всех, кто имеет отношение к предпринимательству и инвестициям в ИТ.

Организатор: РАЭК.

https://2018.rif.ru

27–28 сентября в Казани состоится **IoT World Summit Russia 2018** – самое практическое IoT-мероприятие в России, имеющее мировой масштаб.

IoT World Summit Russia, объединяя международных и отечественных лидеров IoT-рынка и представителей ключевых сфер экономики, помогая создать новые партнерские отношения, которые станут основой для формирования эффективных экологических моделей будущего, ориентированных на человека, будет способствовать технологическому прорыву в сфере IoT в России.

Это мероприятие охватывает множество мировых кейсов по IoT, предоставляет обзоры последних трендов и путей развития индустрии в сегменте интернета вещей и «умных» технологий. На IoT World Summit Russia будут представлены практики по трансформации и автоматизации бизнес-систем.

Ожидается, что в этом году в саммите примут участие делегаты из 24 стран.

Каждый участник найдет интересные для себя потоки по применению технологий в ключевых сферах экономики.

Организатор: Redenex.

http://iotworldsummit.ru

выставки, семинары, конференции

Дата и место проведения, организатор, сайт	Наименование мероприятия
13.06. Москва **Tadviser** www.tadviser.ru/index.php/Конференции_TAdviser	4-я конференция «Big Data и BI Day 2018»
20.06. Москва **Connectica Lab** www.telco-forum.ru	7-й ежегодный форум «Future of Telecom: Business Models & Strategies. Точки роста»
20–22.06. Москва **Quorum** www.quorum.guru/events/hr-meropriyatiya/14th-best-intranet-russia-forum-2018	Национальный форум 14th Best Intranet Russia Forum 2018
09–12.07. Екатеринбург **Минпромторг России** www.innoprom.com	Международная промышленная выставка «ИННОПРОМ-2018: Цифровое производство»
04.09. Алушта **«Академия информационных систем»** www.vipforum.ru/conferences/infobereg	Всероссийский ежегодный форум «Информационная безопасность. ИнфоБЕРЕГ»
13.09. Москва **ИКС-МЕДИА** http://dcforum.ru	**13-я ежегодная международная конференция «ЦОД-2018»**
15.09. Москва **Rusbase, Global Innovation Labs** https://bigdataconf.org	Международная конференция Big Data Conference 2018
26.09. Москва **TAdviser** www.tadviser.ru	Конференция «Оптимизация ИТ-инфраструктуры 2018»
11–13.10. Красноярск **«Красноярская ярмарка»** www.krasfair.ru/events/itCOM	Выставка-форум itCOM-2018

24 и 25 мая в Казани пройдет всероссийская конференция **IT & Security Forum (ITSF)**, которая будет посвящена актуальным тенденциям и новинкам мира информационных технологий, информационной безопасности и решений для повышения эффективности бизнеса.

ITSF – одно из крупнейших событий отрасли информационных технологий и кибербезопасности. Это мероприятие, в котором тематическое содержание и деловые контакты органично совмещены с неформальным общением. Основная цель форума – формирование дружеской коммуникативной среды для профессионалов в области цифровых технологий. К участию в форуме приглашаются руководители ИТ- и ИБ-департаментов, бизнес-подразделений и департаментов АСУ ТП, ведущие специалисты и эксперты, представители крупных компаний нефтегазового, энергетического и промышленного комплексов, а также финансового и государственного секторов.

Организатор: ICL-КПО ВС.

http://itsecurityforum.ru/

24–27 апреля в Москве (ЦВК «Экспоцентр») в рамках Российской недели высоких технологий пройдет 30-я юбилейная международная выставка **«Связь-2018. Информационные и коммуникационные технологии»**.

Выставка «Связь» проводится с 1975 г. и является крупнейшим мероприятием в СНГ и Восточной Европе в сфере телекоммуникаций и информационных технологий. Это витрина отрасли, демонстрирующая передовые достижения и технологии, задающая направление развития рынка на год вперед, удобная демонстрационная и дискуссионная площадка для обсуждения актуальных вопросов, общения профессионалов отрасли, поставщиков и покупателей.

На выставке широко представлены решения для фиксированной, сотовой, спутниковой и волоконно-оптической связи, сетей передачи данных, телекоммуникационное, серверное и сетевое оборудование, системы телевещания для кабельного и спутникового ТВ, радиовещания, специализированное программное обеспечение, решения в области информационной безопасности, виртуализации, интернет-технологии и услуги, решения для e-commerce и др.

Основные тренды выставки связаны с реализацией программы цифровой экономики – 5G, AR&VR, большие данные, искусственный интеллект, робототехника, Индустрия 4.0, дроны и беспилотные системы, облачные технологии, блокчейн, финтех, мобильная экономика, интернет вещей, «умный» город, центры обработки данных. Один из новых разделов выставки – Smart Device Show, в котором демонстрируются решения и технологии в области пользовательской электроники, влияющие на индустрию развлечений, киберспорта и гейминга, рекламы, медиа, здравоохранения, здорового образа жизни и активного отдыха.

В рамках выставки «Связь» традиционно проводится целый ряд деловых мероприятий: XII международный навигационный форум, Большой медиакоммуникационный форум, 22-й международный форум МАС, 2-й «TeleMultiMedia Forum 2018: настоящее и будущее медиапотребления в России и мире», форум «Российский софт: эффективные решения», конференция «IoT: цифровое будущее», конференция операторов связи «GPON и сети доступа 2018: экспертный уровень» и др.

Организатор: «Экспоцентр» при поддержке Минпромторга России, Минкомсвязи России, Россвязи.

www.sviaz-expo.ru

Интернет вещей: первые ростки

Александра Крылова

К всеобщей связности людей, вещей и процессов каждая страна движется по своему маршруту, который строит исходя из технологической готовности промышленности и инфраструктуры. С каких вертикальных рынков начала движение к интернету вещей Россия?

Особенности предложения и спроса на решения в области IoT в 2017 г. стали одной из тем исследований iKS-Consulting и фокусом этой статьи.

Первая скрипка – у государства

Внимание, которое уделяется повышению IQ городских хозяйств во всем мире, вполне объяснимо. Процесс урбанизации будет развиваться по нарастающей. Как прогнозируют в ООН, к 2035 г. в городах будет проживать более 60% населения Земли. Понятно, что вместе с ростом численности жителей увеличится нагрузка на инфраструктуру ЖКХ, транспорта, безопасности, здравоохранения, образования и что готовиться к этому муниципальным властям нужно начинать заранее. В самое ближайшее время им предстоит строить «умные» сети распределения электроэнергии, собирать и в режиме реального времени анализировать данные, характеризующие работу всех городских служб и состояние всех инженерных систем, внедрять интеллектуальное видеонаблюдение с функциями распознавания изображений и т.п.

Как показывает опыт самых известных «умных» городов (в их числе обычно называют Сингапур, Лондон, Барселону и Нью-Йорк), повсеместная установка разнообразных сенсоров и датчиков позволяет не только осуществлять мониторинг отдельных городских инженерных подсистем, ответственных за освещение, распределение и учет потребления ресурсов, но и обеспечить существенную экономию потребляемых ресурсов. Более того, анализ данных позволяет городским властям уже сегодня решать насущные проблемы.

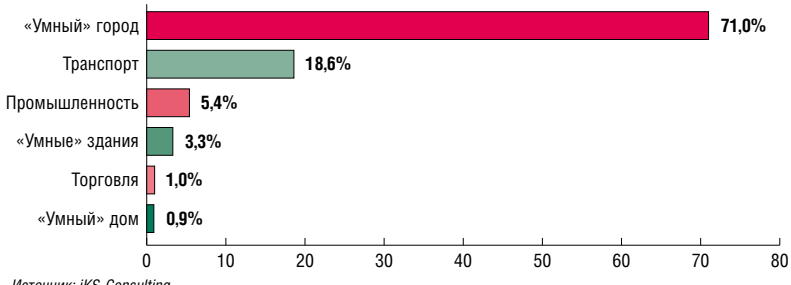
«Умный» город является самым емким сегментом рынка интернета вещей и в нашей стране (рис. 1). Как свидетельствуют результаты исследования iKS-Consulting «Рынок технологий интернета вещей в России – 2017», государство является ведущим потребителем решений на базе технологий IoT. Доля B2G-сектора в структуре пользовательских сегментов интернета вещей, по оценке аналитиков, в 2016 г. превышала 80% (рис. 2).

Ввиду довольно низкого уровня проникновения традиционных систем автоматизации в сферу управления городским и жилищно-коммунальным хозяйством у государства сформировался спрос на программно-аппаратные решения для повышения уровня общественной безопасности и охраны порядка в городах, на интеллектуальные системы для управления дорожным движением и транспортными потоками. Кроме того, государство оказалось заинтересованным в автоматизации учета объектов ЖКХ, в мониторинге их состояния, а также действий служб, ответственных за их эксплуатацию.

К началу 2017 г. в России было реализовано более 100 проектов в области «умного» города, объем рынка в этом сегменте, по данным iKS-Consulting, достиг 63,6 млрд руб. При этом крупнейший сегмент российского рынка интернета вещей практически полностью зависит от государственного финансирования. Государство вкладывает деньги в развитие интеллектуальных транспортных систем, в переоснащение ЖКХ, в системы обеспечения безопасности и здоровья граждан, стремясь развертывать инфраструктуру за счет государственно-частного партнерства.

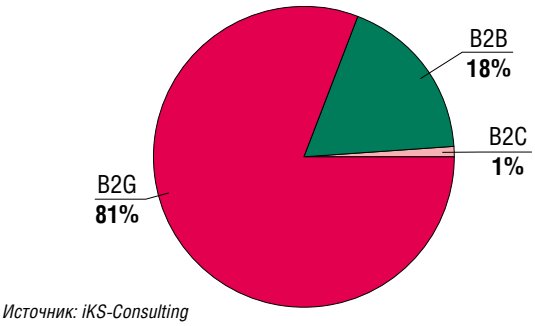
По итогам 2016 г. в такие отношения с государством вступили более десятка компаний – поставщиков типовых решений. Государственно-частные партнерства создавались для распространения интегрированных интеллектуальных решений в области систем безопасности и видеонаблюдения, уличного освещения, а также реализации программы повышения энергоэффективности и распространения практики энергосервисных контрактов.

В качестве примера можно привести проект в области «умного» ЖКХ, реализованный компанией «Центр2М» на магистральных теплосетях дочерней структуры корпорации СТС «Тепло Тюмени». Благодаря технологиям промышленного интернета вещей процесс теплоснабжения можно контролировать как в целом по городу, так и по отдельным категориям социально-значимых объектов. Собираемые данные стекаются в единый диспетчерский центр, получать информацию из которого могут все заинтересованные стороны. Корпорация СТС, вложившая в проект около 30 млн руб., рассчитывает окупить свои инвестиции менее чем за год за счет снижения расходов на эксплуатацию всей теплосети.



Источник: iKS-Consulting

Рис. 1. Структура российского рынка технологий интернета вещей (в денежном выражении) по основным вертикалям, 2016 г.



Источник: iKS-Consulting

Рис. 2. Структура российского рынка технологий интернета вещей (в денежном выражении) по основным пользовательским сегментам, 2016 г.

Родом из M2M

Второй по объему и по уровню развития сегмент интернета вещей в России – «умный» транспорт. Транспортные и логистические компании в нашей стране одними из первых начали использовать телематические (M2M) решения. Установленные в автомобили GSM-модули со встроенными специализированными SIM-картами передают в центр управления информацию об их местонахождении, направлении движения, скорости, расходе топлива и о целом ряде других критичных для бизнеса параметров. В 2016 г., по оценке аналитиков iKS-Consulting, было реализовано более 50 проектов в области «умного» транспорта, поставщиками решений для которых стали более 30 компаний. В 2017 г. объем сегмента «умного» транспорта российского рынка интернета вещей достиг 13,1 млрд руб.

За годы использования M2M-мониторинга на транспорте компании-потребители не просто накопили ценный опыт, но и формализовали технические и организационные процедуры работы с такими решениями, многие из которых продолжают использоваться по сей день. «Технология, основывающаяся на SIM-картах M2M, развивается достаточно стабильно, – констатирует Татьяна Толмачева, партнер iKS-Consulting, – появляются новые заказчики, базовые решения усложняются, в них добавляются востребованный функционал, дополнительная ценность».

По большому счету в сегменте «умного» транспорта у коммерческих компаний, в частности у розничных сетей и промышленных предприятий, сформировался спрос на типовые комплексные ИТ-решения. За право его удовлетворить развернулась серьезная конкуренция между многочисленными поставщиками программно-аппаратных систем, как зарубежными, так и локальными.

Благодаря решению государства о создании в России сначала системы экстренного реагирования при авариях «ЭРА-ГЛОНАСС», а затем и системы «Платон», обеспечивающей взимание платы с грузовиков, которые имеют разрешенную максимальную массу 12 т, транспортные и логистические компании начали переходить от привычного M2M-мониторинга к более сложным интеллектуальным решениям для этого сегмента.

Развитием темы госучастия в стимулировании использования технологий интернета вещей в дорожно-транспортной отрасли можно считать решение об оборудовании автоматических пунктов весогабаритного контроля на всех автомобильных дорогах федерального значения. Его цель – обеспечить сохранность таких трасс путем предупреждения нарушений при движении по ним тяжеловесных и крупногабаритных транспортных средств, оперативное возмещение расходов на ремонт и реконструкцию автодорог, получение данных о грузопотоках в режиме реального времени, а также повышение уровня экологической безопасности.

Согласно Единым техническим требованиям к оборудованию автоматических пунктов весогабаритного контроля, приложенным к распоряжению Росавтодора № 1328-р от 20.07.2016, в каждом таком пункте должны быть развернуты стационарное оборудование и программные средства, обеспечивающие измерение весогабаритных параметров грузовых

МНЕНИЕ ЭКСПЕРТА

Ирина Яхина, директор по технологиям в регионе North EMEA, Hitachi Vantara

Как войти в IIoT

Предприятию, планирующему внедрение решений IIoT, прежде всего необходимо понять, для чего оно внедряет эти решения и каких целей стремится достичь: например, повысить производительность, перевести логистику на новый уровень оптимизации и т.п. Вслед за этим нужно выстроить стратегию развития для того, чтобы получить преимущества от такой цифровой трансформации.

В соответствии с этой стратегией, предприятию предстоит пройти несколько подготовительных этапов. В первую очередь в его распоряжении должны быть устройства и датчики, которые позволяют фиксировать события и параметры оборудования и технологических процессов, предварительно агрегировать и анализировать данные. Для аналитической обработки поступающих с датчиков данных, выполнения и уточнения прогнозных индустриальных моделей ему потребуется внедрить программное решение. Такое решение проектируется и размещается на IIoT-платформе, осуществляющей управление устройствами, а также сбор, предобработку и хранение данных. Кроме того, нужно предусмотреть наличие высоконадежной серверной инфраструктуры и подсистемы безопасности, защищающей от несанкционированных вторжений.

Роль штаба для управления проектами в области индустриального интернета вещей отводится центру знаний и идей – отдельному департаменту, в который должны входить сотрудники как минимум трех подразделений: индустриальные технологи, специалисты по глубинному анализу данных и разработке прогнозных моделей (data scientists), а также ИТ-специалисты (разработчики, специалисты по информационной безопасности).

автомобилей без снижения скорости движения, допустимой на данном участке дороги. Для передачи данных из пункта автоматизированного контроля в АИС, ведущую мониторинг интенсивности и состава транспортного потока, должен использоваться выделенный внешний канал связи с рекомендуемой пропускной способностью 2,5–10 Мбит/с (предпочтительно ВОЛС). Также должна быть предусмотрена возможность обмена по этой линии связи данными с информационными системами органов исполнительной власти, осуществляющими контрольно-надзорные функции.

Очевидно, что участие в этой программе интересно и крупным операторам связи, таким как «Ростелеком», и разработчикам ИТ-решений, в том числе региональным.

От АСУ к IIoT

Несмотря на то что автоматизацией российские предприятия занимаются не одно десятилетие, именно с внедрением решений из области промышленного интернета вещей и с цифровизацией производства эксперты связывают надежды на преодоление технологического разрыва с конкурентами из развитых стран и на оптимизацию производства и сокращение издержек.

Вместе с тем экспертам понятно, что переход от «классической» автоматизации отдельных направлений деятельности предприятия – финансов, логистики, управления человеческими ресурсами и отношениями с клиентами – к типовым программным и аппаратным решениям для комплексного управления технологическими и бизнес-процессами вряд ли будет революционным. «Сегодня на некоторых предприятиях внедряются сложные системы и решения, разработанные под задачи отдельно взятого заказчика, – констатирует Т. Толмачева, – которые в силу своей кастомизированности, по нашему убеждению, нельзя рассматривать как технологии индустриального интернета вещей. К этой категории мы относим типовые решения для автоматизации конкретных процессов бизнеса определенного типа, которые можно с небольшими доработками тиражировать на других предприятиях отрасли».

В качестве примера аналитик приводит АИС «Диспетчер» – универсальную систему мониторинга работы оборудования, персонала и технологических процессов в режиме реального времени, разработанную ИЦ «Станкосервис». Подключать к ней можно любые станки с ЧПУ и другое универсальное оборудование. Как и все системы класса MDC (Machine Data Collection),

Таблица 1.
Готовность к IoT в основных вертикалях

Отрасли / Бизнес-процессы	«Умный» город	Транспорт	Производство	Торговля	«Умное» здание	«Умный» дом
Безопасность и наблюдение						
Управление производством/процессами						
Управление закупками						
Управление запасами						
Управление закупками и поставками						
Управление инфраструктурой						
Управление персоналом						
Повышение энергоэффективности						
Управление автопарком						
Управление отношениями с клиентами						
Управление финансовыми операциями						

Оранжевый: Высокий уровень готовности к IoT, основанный на скорости проникновения традиционных систем автоматизации
Зеленый: Есть практика использования IoT-решений, в том числе реализация пилотных проектов
Серый: IoT-решения не применяются
Источник: iKS-Consulting на основе данных Федерального агентства статистики (2015 г.)

Таблица 2.
Ситуационный барометр рынка IoT в России

Показатели	 Транспорт	 «Умные» здания	 «Умный» город	 Промышленность	 Торговля	 «Умный» дом
Количество проектов, реализованных в 2016 г.	50+	20+	100+	20+	30+	10 000+
Объем рынка в 2017 г., млрд руб.	13,1	2,1	63,6	3,6	0,7	0,6
Среднегодовые темпы роста в 2016–2020 гг., %	14	9	3	8	15	25
Количество поставщиков типовых решений	30+	10+	10+	10+	15+	10+

Источник: iKS-Consulting

АИС интегрируется с системами управления производственными процессами (MES) и управления ресурсами предприятия (ERP) и позволяет оптимизировать загрузку производственных мощностей, сокращать их простои, потери рабочего времени и многое другое.

Заказчики – промышленные предприятия, по мнению Ирины Яхиной из компании Hitachi Vantara, ждут от подобных решений безопасности (зачастую с автоматическим реагированием на основе искусственного интеллекта), высокой доступности и стабильности, а также функциональной эффективности.

Такие комплексные решения в России уже появляются и внедряются: по данным iKS-Consulting, за 2016 г. в этой области было реализовано более 20 проектов. В числе их поставщиков, помимо «Станкосервиса», компании TSOLLA, «ММК-Инжиниринг» и КРУГ. Активность в области промышленного интернета вещей проявляют операторы связи – «Ростелеком», «МегаФон», «Билайн», МТС, системные интеграторы – «Борлас», КРОК, «АйТи», ЛАНИТ и компании, специализирующиеся на разработке решений в области IIoT, такие как Revolta Engineering. В результате объем этого сегмента рынка в денежном выражении на начало 2017 г. оценивался в 3,6 млрд руб.

Появление на рынке типовых решений для объединения в общем информационном поле производственных и управленческих процессов, имеющих в своем составе и сетевую, и платформенную часть, а также средства визуализации собираемых данных, – новый виток эволюции систем автоматизации предприятий. Венцом этого этапа должна стать основанная на технологиях искусственного интеллекта самообучающаяся и самоорганизующаяся инфраструктура, способная действовать с минимальным участием человека или вовсе без него.

Но это в будущем, а пока аналитики отмечают, что промышленный сегмент российского рынка интернета вещей все еще находится на стадии пилотных проектов и экспериментов.

А что же в других отраслях?

Примерно на той же стадии, на перепутье между классической автоматизацией бизнес-процессов, дополненной точечными разработками для мониторинга наиболее важных из них, и внедрением типовых решений в области интернета вещей находятся сегодня в нашей стране и другие вертикальные рынки: «умные» здания, «умный» ритейл и «умный» дом (табл. 1 и 2).

Качественные изменения в «умных» зданиях, их превращение в объекты, вся инфраструктура которых контролируется и управляется из единого центра, сдерживаются консерватизмом девелоперов и неуверенностью инвесторов. Для «умного» ритейла и «умного» дома крайне важен горизонт возврата инвестиций. «Умные» решения в области управления клиентским опытом, анализа поведения покупателей пользуются спросом при условии окупаемости в течение 6–12 месяцев.

Что же касается решений «умного» дома, то их проникновение тормозится нехваткой коробочных предложений, их неоправданной премиальной стоимостью и недостатком продвижения. Преодолев эти сдерживающие факторы, сегмент может, по убеждению аналитиков iKS-Consulting, в период с 2016-го до 2020 г. показать самые высокие среди всех сегментов IoT темпы роста – 25%.

■ ■ ■

Ввиду неравномерного развития сегментов российского рынка IoT в перспективе ближайших четырех лет ему еще предстоит совершить переход от стадии евангелизма и пилотных проектов к разработке и активному продвижению разнообразных типовых plug & play-решений в интересах городского хозяйства, транспорта, промышленности, ритейла, интеллектуальных зданий и жилищ. ИКС

3-я конференция и выставка «ЦОД-2018: модели, сервисы, инфраструктура»

Организатор:

ИКС МЕДИА

31 мая 2018, Казахстан, Алматы, Rixos

Ключевой задачей конференции является обмен мнениями, знаниями и опытом для реализации программы «Цифровой Казахстан». Прежде всего в части развития надежной, доступной, высокоскоростной и защищенной цифровой инфраструктуры.

Цели конференции:

- Повышение капитализации отечественной ИТ-отрасли за счет возможности использования различных форм партнерства, таких как ГЧП, revenue-sharing и др.
- Презентация новых подходов, ИТ-сервисов, решений, возможностей по адаптации существующих продуктов для нужд казахских потребителей
- Развитие сервисных моделей и ИТ-аутсорсинга на рынке Казахстана

Партнер Uptime Institute

www.dcforum.kz

За дополнительной информацией обращайтесь по тел.: +7 (495) 150-64-24, 785-14-90, 229-49-78 и e-mail: dim@iksmedia.ru

Спонсоры и партнеры

Kaspersky Lab · Minimax Fire Products · SUSE · DELL EMC · HITEC Power Protection · АККУ ЭНЕРГО · ОРБИС СОЛЮШНС · PCM Powercom Complete Power Solution · REMER производственная группа

В поисках точек роста

Гузель Куликова

Мысль о том, что инновационная экономика должна прийти на смену сырьевой, много лет звучит с трибуны Гайдаровского форума. В начале года эксперты вновь искали ответ на главный вопрос: как сделать, чтобы цифровая трансформация российской экономики была успешной.

Новые технологии и криптовалюты – в центре внимания российских чиновников, бизнесменов и политиков самых разных уровней. Отношения с блокчейном и искусственным интеллектом здесь складываются непростые: одни ими «болеют», другие боятся и не понимают сути происходящих изменений.

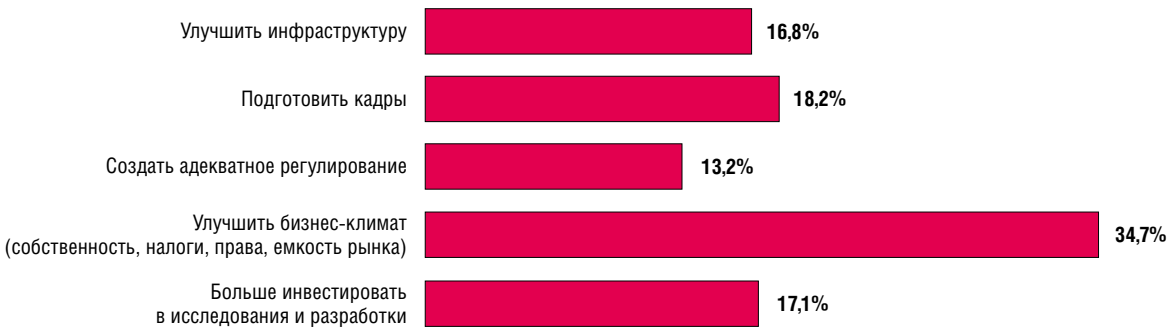
Министр экономического развития РФ Максим Орешкин выделил три технологии, которые повлияют на российскую экономику в ближайшие годы: удаленная идентификация, искусственный интеллект и платформенные решения для электронной торговли и логистики.

М. Орешкин.
На российскую экономику в ближайшие годы повлияют удаленная идентификация, искусственный интеллект и платформенные решения для электронной торговли и логистики

«Удаленная идентификация – это технология, которая будет менять и банковскую сферу, и сферу госуслуг. Она сделает взаимоотношения между контрагентами, особенно с участием физических лиц, гораздо более комфортными и эффективными», – считает министр. Напомним, что в конце 2017 г. Президент РФ Владимир Путин подписал закон, позволяющий с помощью биометрических данных проводить удаленную идентификацию потенциальных клиентов банков. Она будет осуществляться с использованием единой системы идентификации и аутентификации (ЕСИА) и с подтверждением биометрических данных в единой биометрической системе (ЕБС).

От искусственного интеллекта М. Орешкин ожидает в первую очередь повышения эффективности бизнес-процессов: «Если посмотреть на структуру занятости в России и на то, как у нас выстроены различные бизнес-процессы, в том числе на государственном уровне, то мы увидим, что здесь много лишних действий. Внедрение технологий автоматизации и искусственного интеллекта поможет сделать эти процессы эффективными и менее затратными для общества». Третья технология – платформенные решения для электронной торговли и логистики – должна сократить разрыв между конкретным производителем и потребителем товаров в нашей стране и за ее пределами.

К главной теме дискуссии «Бизнес и государство: модели партнерства в цифровую эпоху» обратился председатель правления Сбербанка Герман Греф. Он убежден, что «коллаборация между государством и бизнесом» – это перестройка модели управления. Необходимо вовремя реагировать на происходящие изменения с тем, чтобы «не застыть и не оказаться отброшенными на обочину». Именно поэтому важно выбрать новую модель взаимоотношений между государством и субъектами предпринимательского права. Как показывает опыт, ужесточение регулирования приводит к тому, что бизнес становится изворотливее. «Человек научится докладывать тебе то, что ты хочешь от него услышать. А уж государство с маленькими стартапами, с огромным



Что государство должно сделать в первую очередь для развития цифровой экономики России?

Источник: Центр общественных связей РАНХиГС

количеством субъектов! Если мы дорегулируем до того, что работать им будет некомфортно, они уедут в другие юрисдикции», – предупредил глава Сбербанка. Ключевая задача власти – принять «мягкую» модель регулирования и создавать сопутствующую инфраструктуру.

Кстати, во время интерактивного голосования из ответов на вопрос «Что государство должно сделать в первую очередь для развития цифровой экономики России?» большинство участников дискуссии выбрали предсказуемый вариант: «Улучшить бизнес-климат» (см. рисунок). Как и много лет назад, неприкосновенность бизнеса, гарантии прав на интеллектуальную собственность, налоговый режим волнуют россиян куда больше, чем инфраструктура и инвестиции в исследования и разработки.

Рейтинг инновационных регионов

Россия не первый год ищет возможности для переориентации экспорта с сырья на более высокотехнологичные направления. Речь идет как о развитии перспективных производств, так и о поддержке экспортеров.

Для выявления точек роста Ассоциация инновационных регионов России (АИРР) совместно с Минэкономразвития ежегодно с 2012 г. составляет собственный рейтинг инновационных регионов.

«Мы старались создать рейтинг, который опирался бы на объективные данные и не давал возможности для излишнего субъективизма. Практически по каждому показателю углублялись вплоть до анкет, которыми пользуется Росстат для сбора соответствующей информации», – рассказал Олег Фомичев, статс-секретарь – заместитель министра экономического развития России.

В основе принятой методики – подход, используемый Европейской комиссией для проведения сравнительной оценки инновационного развития регионов Евросоюза. В версию 2017 г. вошел новый показатель – инновационная активность региона, который отражает усилия всех участников системы в применении действующих федеральных инструментов, в привлечении инвестиций и во взаимодействии с государственными институтами развития. Кроме того, он оценивает деятельность местных властей в сфере создания объектов инновационной инфраструктуры.

На протяжении всех лет формирования рейтинга тройка лидеров остается неизменной (табл. 1): Москва, Санкт-Петербург и Татарстан. Правда в текущей версии Санкт-Петербург вышел на 1-е место, а Москва переместилась на 2-е.

В группу сильных инноваторов входят девять субъектов РФ: Томская область заняла 4-е место, Новосибирская – 5-е, Калужская – 6-е, Подмосковье – на 7-й строчке. Впервые в эту группу вошла Ульяновская область, переместившись с 16-го на 8-е место, что обусловлено улучшением ее позиций и по базовым индикаторам рейтинга, и по новым индикаторам инновационной активности региона.

Группу среднесильных регионов составляют 17 субъектов РФ. Здесь яркую динамику продемонстрировала Тюменская область, которая поднялась в рейтинге на 12 позиций. Пример положительного инновационного развития показывает и Новгородская область (+17 позиций), что в основном связано с улучшением значений базовых индикаторов рейтинга.

Таблица 1. Рейтинг инновационных регионов России, 2017 г.

Ранг	Регион	Индекс инновационности	Процент от среднего	Группа	Изменение позиции в рейтинге по сравнению с 2016 г.
1	Санкт-Петербург	0,71	183,8%	Сильные инноваторы	1
2	Москва	0,69	179,3%		-1
3	Республика Татарстан	0,66	173,3%		0
4	Томская область	0,63	163,9%		0
5	Новосибирская область	0,57	148,5%		0
6	Калужская область	0,55	143,8%		0
7	Московская область	0,55	142,8%		2
8	Ульяновская область	0,55	142,5%		8
9	Самарская область	0,54	142,0%		1
10	Тульская область	0,52	135,9%	Среднесильные инноваторы	2
11	Нижегородская область	0,52	135,1%		-3
12	Республика Башкортостан	0,52	134,5%		-5
13	Республика Мордовия	0,52	134,4%		1
14	Тюменская область (без АО)	0,50	131,4%		12
15	Ярославская область	0,50	131,2%		5
16	Красноярский край	0,50	130,6%		-5
17	Свердловская область	0,50	129,0%		-4
18	Пермский край	0,49	126,7%		-3
19	Воронежская область	0,48	123,9%		-2
20	Чувашская Республика	0,47	121,9%		3
21	Липецкая область	0,46	120,5%		-3
22	Челябинская область	0,45	117,4%		-1
23	Новгородская область	0,43	112,7%		17
24	Рязанская область	0,43	112,4%		6
25	Пензенская область	0,43	111,4%		-1
26	Владимирская область	0,43	111,3%		-4

Примечание: приведены данные по двум группам – среднесильные и сильные новаторы.

Источник: по данным АИРР

Достоинства и ограничения рейтинга проанализировал главный научный сотрудник Центрального экономико-математического института РАН Олег Голиченко. Он отметил, что прямая связь исследователей с госучреждениями и инновационными предприятиями, предоставившими информацию, – большое достоинство рейтинга. Вместе с тем из исследования «выпали» средние предприятия, хотя именно они очень активны в инновационной деятельности. На данный момент рейтинг отражает лишь общую картину, созданную «крупными мазками».

Центры притяжения

Более детальный анализ был представлен в национальном докладе «Высокотехнологичный бизнес в регионах России», подготовленном РАНХиГС и АИРР совместно с группой «Интерфакс». Цель исследования – определить потенциальные точки несырьевого роста российской экономики на основе анализа региональной структуры и тенденций развития высокотехнологичного бизнеса за 2010–2016 гг.

По мнению авторов, система индикаторов дает представление о том, где выгодно вести бизнес и какие регионы в этом преуспели. В числе ключевых условий – ресурсы капитала, труда, институциональная среда, инфраструктурная обеспеченность и научный потенциал регионов (табл. 2).

Таблица 2. Оценка значимости условий развития высокотехнологичными компаниями

Блок условий из рейтинга	Фактор, обозначенный в анкете	Средняя оценка значимости респондентами (от 0 до 1)	Средний весовой коэффициент блока в рейтинге (от 0 до 1)
Капитал	Доступ к инвестициям	0,45	0,25
Кадры и привлекательность региона	Доступность трудовых ресурсов необходимой квалификации	0,15	0,2
	Климат в регионе	0,39	
	Комфортность проживания	0,53	
Институты	Число и интенсивность проверок	0,64	0,25
	Жилье и социальная инфраструктура	0,39	
	Доступ к негосударственным услугам	0,49	
	Неформальные платежи	0,28	
Научный потенциал	Доступ к технологиям	0,19	0,1
Инфраструктура	Доступ к базовой инфраструктуре	0,11	0,15
	Доступ к инновационной инфраструктуре	0,49	

Источник: «Высокотехнологичный бизнес в регионах России», РАНХиГС, АИРР, группа «Интерфакс»

«Основная проблема в развитии высоких технологий в России – нехватка кадров. Квалифицированные кадры продолжают покидать нашу страну, – с горечью констатировал старший научный сотрудник РАНХиГС Степан Земцов. – Сейчас, по нашим оценкам, в высокотехнологичном секторе занято примерно 15 млн человек, но эта цифра постепенно уменьшается». Вместе с тем более 20% сотрудников hi-tech-предприятий работают в трех регионах: Москва, Подмосковье и Санкт-Петербург. На основе анализа данных о миграции высококвалифицированных специалистов были оценены наиболее значимые региональные факторы, способствующие привлечению специалистов.

Сегодня центрами притяжения креативного класса являются Подмосковье, Татарстан, Санкт-Петербург, Воронежская, Белгородская, Тюменская, Липецкая, Ленинградская, Нижегородская области и Москва. Аналитики обращают внимание на то, что привлекательность столицы снижается (индекс упал с 0,84 в 2007 г. до 0,71 в 2016 г.). Данный тренд связан с соотношением доходов и прожиточного минимума. Это дает возможность другим регионам переманить кадры путем организации новых производств, создания должной инфраструктуры, повышения доступности жилья и комфортности проживания. Комфортность проживания представители бизнеса считают важным фактором, наряду с интенсивностью проверок и доступом к капиталу. Совет особенно актуален для руководителей районов с теплым климатом.

Вместе с тем один из наиболее значимых показателей развития высокотехнологичного бизнеса – создание стартапов. В 2016 г. было создано 64 907 технологических стартапов, что на 21% больше, чем в 2010 г; в совокупности за период 2010–2016 гг. в стране появилось 409,4 тыс. молодых технологических компаний.

Аналитики констатируют, что рост технологического предпринимательства тесно связан с развитием инфраструктуры региона. В данном аспекте лидирует Татарстан. В Тюменской области драйверами роста инновационных предприятий являются высокая концентрация капитала, масштабные инвестиционные проекты, требующие субподрядчиков, и увеличение госзакупок.

«Есть много регионов, где сложились хорошие условия и есть ресурсы для развития высоких технологий», – подвел итоги С. Земцов. Авторы доклада считают, что их труд может быть использован как аналитический инструмент для развития технологий в структуре региональных экономик.

Надежды на помощь государства

В 2016 г. в рамках политики инновационного развития экономики запущен новый проект «Национальные чемпионы», призванный вырастить за несколько лет более 10 российских частных высокотехнологичных компаний с объемом продаж не менее $500 млн каждая. К концу

2020 г. половина компаний-участниц обязана нарастить объем высокотехнологичного экспорта в четыре раза, как минимум две компании должны выйти на объемы продаж в $1 млрд в год и не менее десяти – $500 млн в год.

Напомню, что на первом этапе было отобрано 30 компаний-лидеров, которым на протяжении 2017 г. оказывалась индивидуальная информационно-консультационная поддержка, помощь во взаимодействии с органами власти и институтами развития, госкомпаниями, в продвижении на зарубежных рынках с привлечением торговых представительств РФ.

На втором этапе в 2017 г. в проект вошли 32 новых участника, в числе которых 13 компаний, работающих в сфере ИКТ. Многие из них хорошо известны на нашем рынке: «ИнфоВотч», «ИнфоТеКС», «Лаборатория Касперского», «Эйдос-Медицина», Лаборатория «Вычислительная механика».

Директор департамента стратегического развития и инноваций Министерства экономического развития РФ Артем Шадрин подчеркнул, что усилия институтов развития сконцентрированы на лидерах рынка, которые уже доказали свою конкурентоспособность и умеют наращивать объемы продаж и производства: «Здесь мы говорим в первую очередь о поддержке по линии экспорта (Российский экспортный центр), создании новых мощностей (Фонд развития промышленности). Также рассчитываем, что в этом году эффективно подключатся Внешэкономбанк и "ВЭБ Инновации"». Помощь планируют оказывать и федеральные министерства, например, Минобрнауки выделит субсидии на НИОКР. Отдельным направлением станет работа по вовлечению «чемпионов» в Национальную технологическую инициативу, чтобы бизнес мог воспользоваться мерами поддержки в рамках НТИ. Среди задач проекта – помощь высокотехнологичным компаниям в выходе на рынок капитала, проведение IPO и размещение облигаций. Стоит отметить, что из 62 компаний, входящих в проект, 24 – московские, 12 – из Санкт-Петербурга, четыре – из Московской области, три компании – из Томской области и по две компании пришлось на Татарстан, Новосибирскую область и Пермский край.

Отбор компаний в проект осуществляется на базе рейтинга «ТехУспех», который разработан Российской венчурной компанией в партнерстве с НИУ ВШЭ. Анкетный опрос участников проекта «Национальные чемпионы», проведенный разработчиками рейтинга, показал, что в ближайшие пять лет высокотехнологичные компании планируют прежде всего наращивать компетенции, связанные с разработкой и коммерциализацией новых продуктов, а также совершенствовать производственные процессы. Уже сегодня почти 74% опрошенных компаний действуют на внешних рынках и только 5% не планируют экспортировать свою продукцию. Работа на внешних рынках, по мнению 28% респондентов, позволяет подтвердить конкурентоспособность продукции в глазах отечественных потребителей, 22% компаний отметили, что поставки на экспорт ведутся много лет и являются традиционным направлением деятельности, а 21% опрошенных рассматривает экспорт как средство преодоления ограниченности внутреннего рынка.

По сравнению с 2016 г. произошел сдвиг. Компании больше ожидают господдержки и учитывают ее в своих планах: 39% компаний считают, что без помощи государства часть запланированных показателей не будет достигнута. В 2016 г. такой позиции придерживалось 20% компаний. Бизнес ждет от государства уже не только финансовых ресурсов, но и административной помощи для решения вопросов в органах власти, организации бесплатных образовательных программ для переподготовки кадров, а также получения консультаций при выходе на иностранные рынки. На софинансирование со стороны государства они рассчитывают и в проведении своих будущих НИОКР.

Г. Греф:
«С 2000 по 2017 гг. стоимость выхода интернет-стартапа на рынок уменьшилась в 1000 раз: в 2000 г. она составляла $5 млн, а сегодня – $5 тыс.»

С точки зрения Александра Идрисова, основателя Strategy Partners Group, у большинства участников есть хорошая возможность для дальнейшего роста и развития. Однако «национальные чемпионы» недооценивают свой потенциал роста. Он вспомнил, как при запуске проекта у многих компаний-участниц были сомнения: «Может быть, нам тихо посидеть и подождать, когда станет поспокойнее?». «Мы им говорим, что вашим детям не нужны "заводы-пароходы", им нужны ликвидные акции. И то, что сегодня начал развиваться фондовый рынок – это выход для большинства владельцев бизнеса», – резюмировал эксперт.

Особенности реализации проекта в 2018 г. – фокус на новые рынки НТИ, вовлечение в осуществление программы «Цифровая экономика РФ», формирование новых механизмов привлечения инвестиций (краудфандинг, краудлендинг). Хочется верить, что проект не превратится в очередной пшик, а станет действенным инструментом поддержки частного бизнеса со стороны государства. ИКС

Save to reinvest как стратегия успешного развития

О том, как заставить цифровой актив приносить реальную прибыль бизнесу и не «сгореть» в гонке за новыми технологиями, – Евгений Ягнятинский, директор по информационным технологиям компании Procter & Gamble в Восточной Европе и Центральной Азии.

Евгений Ягнятинский

На пересечении настоящего с будущим

– По прогнозам специалистов, самыми перспективными технологиями в 2018 г. станут квантовый компьютинг, искусственный интеллект, биометрия и решения, обеспечивающие кибербезопасность. Евгений, какие из этих технологий актуальны для развития бизнеса Procter & Gamble?

– В нашей компании мы рассматриваем технологии в контексте того, что они могут дать для развития бизнеса. Поэтому я не буду оценивать квантовый компьютинг и биометрию. Уверен, по мере того, как они начнут действительно входить в жизнь, появятся интересные инструменты на их основе для решения практических задач. А вот искусственный интеллект – да, технология для нас однозначно актуальная. Мы применяем ИИ для работы с данными и обмена ими как внутри компании, так и с нашими партнерами по медиабизнесу, ритейлу.

Кибербезопасность – важная для нас задача, в первую очередь с точки зрения уязвимости информационных технологий производства. Офисные системы защищены лучше, поскольку платформы, на которых работаем: майкрософтовские, гугловские и т.д., – постоянно отслеживают ситуацию, делают патчи, информируют о возникших угрозах. Производственная же зона, которая тоже по своей сути ИТ-система, требует специализированных средств защиты.

– Если я вас правильно поняла, в фокусе компании прежде всего апробированные решения.

– Для нас как для фирмы, которая работает с потребителем, более интересны технологии настоящего или находящиеся на пересечении настоящего с будущим. На мой взгляд, даже потенциал простых мобильных решений пока не используется полностью. В России много говорят об omni-channel retail (интегрированном подходе к покупателю), но по большому счету здесь еще много пространства для эксперимента. Например, технологии виртуальной и дополненной реальности мы уже пробовали.

– Какие бизнес-задачи помогают решать проекты на основе виртуальной реальности?

– Для нас важно знать своего потребителя, уметь правильно его понимать, доносить до него информацию, скажем, о том, чем интересен тот или иной продукт, как им пользоваться. Узнать не со слов, а из наблюдений за человеком, какое место этот продукт может занять в его жизни и насколько хорошо удовлетворяет запросы. И виртуальные системы используются для исследования потребительских предпочтений, поведенческих схем. В частности, инструмент позволяет понять, как наши потребители реагируют на разные типы упаковок, расположение товаров определенных марок на полках магазинов. С помощью технологии виртуальной реальности мы также тестируем новые формы продуктов – крышек для бутылок, разнообразных дозирующих устройств. Раньше для этих целей выпускали небольшое количество нового товара, выкладывали его на полках магазинов, привлекали фокус-группы. Исследования потребительских предпочтений помогают выстраивать работу с владельцами торговых центров, ведь мы можем им рассказать не только о товаре, но и о предпочтениях покупателей.

Вторая область применения технологии – взаимодействие с нашими ритейл-партнерами. Мы предоставляем им возможность увидеть, как в конкретной торговой сети могут быть установлены информационные дисплеи, изменен дизайн, расставлены товары на витринах и т.п. Проводить такие апробации в магазинах – задача непростая, а виртуальная реальность существенно экономит и время, и деньги.

– Вы упомянули мобильные технологии, могли бы рассказать о них подробнее?

– Я остановлюсь на голосовых решениях. Думаю, что они станут отличным инструментом формирования лояльности клиентов. Приведу конкретный пример. Сегодня голосовые ассистенты интегрируются во все, что «живет» в мобильном телефоне: календарь, различные мессенджеры, и молодежь открыта таким решениям, поэтому появляются новые сценарии взаимодействия.

В ноябре 2017 г. мы провели хакатон для студентов на тему «Научи известные марки говорить» с целью попробовать применить голосовое общение к решению бизнес-задач – реклама, продажи, консультации потребителя и т.д. Участники выдвинули интересные идеи о том, как построить общение с потребителем, чтобы при возникновении бытовых проблем он обращал внимание на продукты наших брендов. Скажем, в случае обращения: «Ой, пролил вино на рубашку» голосовой помощник мог бы рекомендовать продукт и способ стирки, способный решить задачу. Эксперименты с новыми технологиями позволяют нашим маркам быть интересными новому поколению.

Не количество, а качество

– Как ИТ-директору подготовить компанию к цифровой трансформации?

– Я не могу сказать, что был период, когда цифровой трансформации не было, а потом она вдруг появилась. Просто градус постепенно повышается: становится все жарче и жарче. Внимательно наблюдаешь за происходящим вокруг, чтобы понимать, какие тренды действительно открывают новые возможности для развития бизнеса, а какие – очередной мыльный пузырь.

– Пришлось ли вам в последние два-три года вносить существенные коррективы в ИТ-стратегию и ИТ-бюджет в связи с новыми тенденциями?

– Да. С точки зрения ИТ-стратегии были аспекты, к которым пришлось изменить подход. Поскольку технологии все время дешевеют и вытесняются новыми, более простыми и удобными, то инвестиции в ИТ всегда могут быть оптимизированы. Обычно в больших компаниях все происходит так: «Хотим новую технологию! Руководство, дайте больше денег!». Сегодня же часть нашей стратегии – save to reinvest, т.е. прежде чем вливать дополнительные средства в новации, нужно оптимизировать существующие расходы и учиться использовать то, что уже есть. Вместе с тем мы смотрим, можно ли перераспределить ресурсы: забрать из того сегмента решений, который по сравнению с другими в наименьшей степени задействован в бизнес-процессах.

Второй момент, в который внесена корректива, – это скорость получения прибыли от инвестиций. В начале 2017 г. в компании было запущено порядка 80–90 проектов, связанных с внедрением технологий. Понятно, что организация не в состоянии «переварить» такое количество новых идей сразу, поскольку нужно заниматься ежедневно бизнесом и невозможно одновременно координировать изменения в 80 аспектах бизнес-процессов таким образом, чтобы они эффективно работали.

Чтобы технологии приносили реальную прибыль, нужно ограничить количество новых проектов и сконцентрироваться на их правильном и быстром внедрении. Если у «пилота» нет положительного результата, он затягивается, то его нужно безжалостно «убивать» и переходить к новому проекту. Новации должны иметь конкретную ценность для компании.

Да, конечно, есть желание работать в экспериментальном режиме, однако на практике чем больше технологий в операционном портфеле, тем сложнее их поддерживать и управлять ими. Поэтому третий аспект стратегии – пусть технологий будет меньше, но они будут самыми эффективными именно для нашей компании. В итоге об успехе новой технологии судят по тому, смогла ли она стать частью бизнес-процесса или используется как подсобный инструмент.

Наш footprint в России небольшой

– Сколько у вас дата-центров? Где они расположены?

– Как у глобальной компании у нас два дата-центра за границей: один находится в США, другой в Азии. Все наши бизнес-процессы централизованно реализуются в этих структурах. Исключение – хранение и обработка данных, регулируемые, например, российским законодательством. Поэтому наш footprint, как говорят в ИТ, в России небольшой.

– Используете ли вы сервисы коммерческих ЦОДов?

– Да, поскольку мы строго придерживаемся российского законодательства: для обработки персональных данных мы используем российский ЦОД. Но, опять же, у нас есть глобальные партнеры по инфраструктуре, которые в общем пакете услуг подбирают для нас соответствующие решения. В этом вопросе мы полагаемся на их компетенции, и у меня нет необходимости выбирать на отечественном рынке «самый правильный» ЦОД самостоятельно.

– Применяете ли вы облачные технологии?

– Конечно. Например, у нас много веб-сайтов, на которых представлены наши торговые марки. Для таких решений гораздо дешевле, удобнее и целесообразнее задействовать облачные технологии. Стоит отметить, в облаке мы не хра-

ним персональные данные, «не прошиваем» тяжелую бизнес-логику.

С другой стороны, система ERP у нас пока размещена в наших дата-центрах. Хотя мы реализуем проект, который позволил бы использовать для этого облако. Удастся ли получить финансовый результат? Здесь положительный ответ не столь очевиден. Мы апробировали схему в частном облаке, однако «пилоты» показали, что экономия мизерная, тогда как расходы по проведению трансформации значительные.

Мы пробовали переносить в облако отдельные модули: те из них, которые связаны, в частности, с работой наших заказчиков или поставщиков, получались лучше. Однако появилось много вопросов, которые нужно решать во всех процессах обмена данными между разными модулями. Да, есть возможность сэкономить на инфраструктуре, в числе преимуществ – доступность и надежность, однако и усилия, затрачиваемые на перенос в облако, немалые. Нужно создавать новые интерфейсы, налаживать новые процессы, и все это на живом организме. Поэтому облако мне представляется прежде всего способом внедрения новых процессов или полной трансформации старых. Модернизация существующих решений и процессов на облаке – это довольно сложные проекты-внедрения, и финансовые показатели очень индивидуальны: иногда такие проекты имеют смысл, а иногда и нет.

> Когда слово «облако» видишь на бумаге, оно выглядит замечательно, а в реальности нужно садиться и считать.

– Слабое звено облачных технологий – безопасность. Как вы решаете эту проблему?

– Безопасность – один из факторов, в силу которого многие наши приложения до сих пор остаются в ЦОДах и не переносятся в облако. Хотя с нашими облачными провайдерами (мы в основном работаем с Microsoft Azure и Amazon Web Services) нам удалось построить разумные решения с высоким уровнем защиты, где облачные компоненты и взаимодействия дополнены протоколами безопасности специально для наших сценариев внедрения. Да, они нам позволяют уже сейчас переводить и в Azure, и в AWS определенные решения, которые связаны в том числе с информацией ограниченного доступа, персональными данными. Однако это потребовало сотрудничества на уровне высшего руководства компаний и существенных расходов. Иными словами, когда слово «облако» видишь на бумаге, оно выглядит замечательно, а в реальности нужно садиться и считать.

– Модная сегодня тема – интернет вещей. Используете ли вы соответствующие решения?

– Да, для нашей компании эта тема началась три-четыре года назад. Мы с коллегами тогда дискутировали на тему интернета вещей в бизнесе, и оказалось, что независимо друг от друга все стали пробовать запрограммировать набор датчиков для сценария, связанного с резервированием комнат для совещаний. На сегодняшний день мы внедрили такие решения во многих офисах компании. Установили в переговорных датчики, позволяющие определить, занята комната или свободна. А централизованная система дает возможность в режиме реального времени забронировать свободную комнату и проинформировать сотрудников о том, что она занята. Но это было, что называется, на заре данной технологии, а сейчас портфель применений очень большой.

– Есть ли интересные идеи применения технологии для потребителей?

– Для нас интернет вещей – инструмент, который помогает лучше узнавать наших потребителей за счет той информации, которой они готовы с нами поделиться. Приведу пример. Несколько лет назад мы запустили в производство электрическую зубную щетку с интерфейсом Bluetooth и приложения к ней для основных мобильных платформ. Позиционные и динамические датчики позволяют отслеживать положение щетки в полости рта и подсказывают, где еще надо почистить зубы. Первая версия была очень простая, в сегодняшней версии используются методы геймификации, появляется элемент дополненной реальности, что нравится и детям, и взрослым. Для потребителя польза в том, что благодаря полученной с помощью устройства и приложения информации они более правильно поддерживают гигиену рта. Мои дети стали с удовольствием чистить зубы рекомендованные две-три минуты.

Мы же получаем данные от сенсоров, которые используем для аналитики. Такая информация позволяет понять, какие изменения можно внести в конструкцию прибора и т.д. Это выгодно с точки зрения роста лояльности потребителей, потому что продукт помогает им решать насущные проблемы. Вместе с тем, основываясь на нуждах потребителя, мы смогли продавать больше сопутствующих гигиенических средств.

Сегодня мы экспериментируем с разными решениями. Наши сотрудники на внутреннем хакатоне придумали, как встроить сенсоры в упаковки со стиральными порошками: продукт «приглядывает» за процессом стирки и вовремя напоминает о том, что пора разгрузить стиральную машину или что пришло время купить новую упаковку стирального средства.

Беседовала Гузель Куликова

Стоимость подрядных работ в ЦОДе: как правильно согласовать?

Нередко от того, насколько корректно в договоре определены стоимость поручаемых подрядчику работ и порядок их оплаты, зависит непрерывность функционирования ИТ-оборудования заказчика.

Сергей Смолин, заместитель руководителя юридического департамента, DataSpace

В процессе пользования услугами дата-центра клиент нередко сталкивается с необходимостью проведения дополнительных работ в отношении своего оборудования, размещенного в ЦОДе: могут потребоваться установка и подключение серверных стоек, изоляция холодного коридора, строительно-монтажные и пусконаладочные работы в машинном зале и пр. Как правило, для проведения подобных работ клиент прибегает к помощи специализированного подрядчика или же непосредственно оператора ЦОДа.

Одно из важных условий договора подряда на выполнение каких-либо работ в ЦОДе – определение их стоимости. Если соглашение сторон о цене работ, порядке ее изменения и порядке оплаты не будут надлежащим образом отражены в договоре, заказчик рискует заплатить за работы значительно больше, чем планировал. По этой причине в договоре с подрядчиком цена работ и порядок оплаты должны быть зафиксированы максимально подробно.

При согласовании с подрядчиком объема работ клиент ЦОДа должен также стремиться к минимизации риска перерывов в функционировании своего оборудования. Это означает, что обо всех условиях выполнения работ клиент ЦОДа должен договориться с подрядчиком до их начала. Более того, необходимо учесть все факторы, которые могут на эти работы повлиять, и соглашение о цене работ входит в число таких факторов.

Определение стоимости работ в дата-центре

Глава 37 Гражданского кодекса РФ регламентирует основные требования к согласованию цены в договоре подряда. Стоимость работ может быть твердой, заранее установленной сторонами, или приблизительной, определяемой только в процессе выполнения работ. При заключении договора подряда стороны преимущественно прибегают к твердой стоимости работ. Это позволяет заказчику оставаться в рамках выделенного бюджета. Ситуации, когда стоимость работ в ЦОДе определяется приблизительно, встречаются намного реже – у заказчика и подрядчика, как правило, есть возможность просчитать стоимость проекта заранее.

Документом, в котором подрядчик фиксирует стоимость работ, является смета. При заключении договора на проведение работ в дата-центре заказчик особое внимание должен уделить согласованию сметы, предложенной подрядчиком. На основании данного документа заказчик вправе требовать от подрядчика выполнения перечисленных в смете работ и использования указанных материалов. В силу определенной специфики работ в ЦОДе необходимо корректно и подробно описать в смете объем и стоимость работ и используемых материалов. В противном случае заказчик рискует получить плохо выполненную работу с некачественными материалами.

Тем не менее ст. 709 ГК РФ допускает заключение договора подряда без сметы. Более того, если смета не будет согласована и подписана заказчиком работ, то подрядчик не вправе ссылаться на нее при возникновении конфликта с заказчиком.

В случаях, когда работы с оборудованием клиента производятся силами оператора ЦОДа, риск некорректного составления сметы практически отсутствует – оператор как непосредственный владелец дата-центра обычно имеет четкое представление об объемах и стоимости выполняемых работ.

Изменение стоимости договора в процессе производства работ

Фиксация стоимости работ в договоре не всегда означает, что эта стоимость будет окончательной. В некоторых ситуациях цена изменяется уже в процессе выполнения работ. В одних случаях заказчик может предвидеть такое изменение, а в других изменение цены становится для него неожиданностью. Рассмотрим основные причины изменения стоимости работ после подписания договора.

- Согласованное сторонами изменение стоимости работ. Заказчик и подрядчик имеют право заключить дополнительное соглашение к договору подряда, в котором могут пересмотреть объем работ или используемых материалов, а также их стоимость. Например, в процессе изоляции холодного коридора в машинном зале заказчик решил установить еще несколько серверных стоек в рядах,

При согласовании с подрядчиком объема работ клиент ЦОДа должен также стремиться к минимизации риска перерывов в функционировании своего оборудования.

что потребует выполнения дополнительных работ с использованием дополнительных материалов. При заключении дополнительного соглашения действуют те же правила, что и при согласовании договора. Заказчику необходимо учитывать риск того, что подрядчик может отказаться от увеличения объема выполняемых работ или, понимая важность их результата для клиента, значительно повысить цену. В подобной ситуации наиболее комфортным для клиента подрядчиком является оператор ЦОДа, поскольку он, как правило, не ставит себе целью получение разовой прибыли вследствие сложной ситуации клиента.

- Изменение курса валют. При проведении работ в дата-центре часто используются материалы и оборудование иностранных производителей, которые заказываются из-за рубежа. Стоимость таких материалов и оборудования фиксируется в иностранной валюте. По этой причине подрядчики обычно вносят в договоры условие об одностороннем изменении цены работ в случае резкого изменения курса валюты по отношению к рублю. Таким образом подрядчик за счет заказчика страхует себя от риска переплаты за заказанные материалы и оборудование. Например, стороны согласуют работы по установке в машинном зале дата-центра датчиков температуры, которые подрядчик самостоятельно приобретает у иностранного производителя. Цена договора фиксируется, но также оговаривается, что стоимость материалов может быть увеличена в случае изменения курса доллара, установленного Центральным банком РФ, более чем на 3% по отношению к рублю на дату подписания договора. Если в процессе поставки оборудования курс доллара вырастет, скажем, на 5%, подрядчик вынужден заплатить за датчики больше, чем планировал, и соответственно свои убытки он закладывает в цену договора с заказчиком, увеличивая ее. Для клиента ЦОДа такой порядок изменения цены заключает в себе риск возникновения дополнительных расходов. При выполнении подрядных работ оператором ЦОДа риски последующего изменения цены договора снижаются – как правило, оператор располагает определенным запасом необходимых материалов и оборудования, а большие объемы поставок значительно уменьшают для него их конечную стоимость.
- Непредвиденные работы. В соответствии с пп. 5 и 6 ст. 709 ГК РФ, подрядчик может требовать повышения цены договора при возникновении непредвиденных расходов, увеличении объема работ или значительном росте стоимости материалов. Такое увеличение цены договора не является односторонним – заказчик должен дать на него свое согласие. В случае отказа договор расторгается, и подрядчику оплачивается только фактически выполненный объем работ. Если же в качестве подрядчика выбирается оператор ЦОДа, вероятность возникновения непредвиденных работ сводится к нулю, поскольку оператор ЦОДа является наиболее информированной стороной в вопросе корректного определения объема необходимых работ.
- Экономия подрядчика. Ст. 710 ГК РФ регулирует ситуацию, когда подрядчик при реализации проекта сумел уменьшить расходы на работы или материалы. В этом случае подрядчик может претендовать на согласованную цену договора несмотря на то, что он понес меньшие расходы. Однако экономия подрядчика не должна отразиться на качестве работ. Например, если при установке антенны клиента на крыше дата-центра подрядчик использует материалы более дешевые, но с требуемыми характеристиками, то разница в цене этих материалов составит выгоду подрядчика. Но если характеристики материалов будут хуже требуемых, подрядчик обязан или устранить недостатки за свой счет, или возвратить разницу в стоимости материалов. Такая модель экономии несет определенные риски для заказчика, поэтому все необходимые характеристики материалов необходимо отражать в договоре или смете.

Также в договоре можно указать, что в случае экономии подрядчика сэкономленные средства остаются у заказчика. Это поможет стимулировать подрядчика выполнять работы строго в соответствии с условиями договора.

Аванс или постоплата?

При согласовании договора на производство работ стороны фиксируют порядок оплаты – это может быть аванс, поэтапная оплата, постоплата и т.д. Часто подрядчики требуют частичной или полной оплаты работ авансом, что заключает в себе определенные риски – подрядчик может отказаться от выполнения работ, выполнить их некачественно или не полностью, а заказчик будет вынужден тратить ресурсы на полный или частичный возврат аванса. Для уменьшения таких рисков в договоре следует указывать, что частичный аванс перечисляется за стоимость материалов и эти материалы становятся собственностью заказчика уже в процессе работ. Как правило, стоимость используемых материалов велика и составляет большую часть цены договора.

Например, клиент ЦОДа заключил договор на установку дополнительных камер видеонаблюдения в машинных залах. По условиям договора он выплачивает подрядчику аванс, который покрывает стоимость камер. Даже если по вине подрядчика возникнут сложности с проведением работ, у клиента в собственности останутся камеры видеонаблюдения. Такая модель взаимодействия помогает в определенной степени сохранить бюджет заказчика и снизить расходы на урегулирование конфликта с подрядчиком.

При реализации крупных проектов, например смены оператора ЦОДа с перемещением оборудования клиента в другой дата-центр, рекомендуется оплачивать работы поэтапно, по мере их фактического выполнения.

Еще один способ оплаты работ – применение почасовой ставки. Как правило, такая модель используется подрядчиком в случае проведения многочисленных небольших работ в ЦОДе. Например, клиент дата-центра планирует начать эксплуатацию нового машинного зала. В процессе эксплуатации у него может возникнуть необходимость в установке того или иного дополнительного оборудования. В этом случае клиенту удобнее зафиксировать стоимость одного часа работы сотрудников подрядчика, а после выполнения всех работ оплатить фактически затраченное ими время. Основной риск в такой модели взаиморасчетов – возможность завышения подрядчиком количества затраченных человеко-часов, поэтому ход работ необходимо контролировать.

При согласовании договора с привлеченным подрядчиком у клиента ЦОДа могут возникнуть сложности с определением порядка оплаты – не многие подрядчики согласятся проводить работы на условиях постоплаты. Если же работы проводятся оператором ЦОДа, то стороны могут согласовать комфортный для клиента порядок оплаты, поскольку между ними уже есть действующий контракт на предоставление услуг дата-центра, что значительно облегчает переговорный процесс.

■ ■ ■

Таким образом, при проведении работ в отношении своего оборудования, размещенного в дата-центре, клиент ЦОДа в первую очередь должен предусмотреть в договоре подряда условия, которые касаются минимизации рисков, связанных с изменением цены договора в процессе работ. В противном случае сложности при согласовании с подрядчиком изменения стоимости могут привести к нарушению непрерывности функционирования оборудования клиента.

Стороны должны максимально подробно и корректно зафиксировать в договоре связь между предметом работ и их стоимостью. Это гарантирует клиенту ЦОДа сохранение бюджета – каждый отдельный этап работы оценен, и в случае выявления недостатков он вправе требовать от подрядчика их устранения или соразмерного уменьшения цены договора. Если изменение стоимости работ невозможно предвидеть по объективным причинам, клиенту ЦОДа следует определить в договоре способ оперативного согласования изменения цены. Это уменьшает риск остановки работ и дает заказчику определенную свободу в корректировке процесса. Важную роль играет профессиональный технический и юридический менеджмент всего процесса, начиная с этапа согласования договора на проведение работ и заканчивая приемкой выполненных работ и последующим использованием результатов.

Если клиент дата-центра не готов к риску непредвиденного увеличения стоимости работ или сроков ее выполнения, то наиболее надежным подрядчиком для него становится оператор ЦОДа. В этом случае затраты времени и средств на согласование проекта работ значительно уменьшаются и вместе с тем уменьшается риск ошибочного определения стоимости работ. Имея полное представление о характеристиках дата-центра, оптимальных вариантах выполнения работ и обладая необходимой квалификацией, оператор ЦОДа может предложить клиенту наиболее комфортные условия договора, а проверенная база поставщиков и наличие склада оборудования гарантируют, что его цена не подвергнется изменению. ИКС

Edge Computing: из облаков на землю

Николай Носов

Перенесение вычислений максимально близко к источнику данных позволяет устранить многие недостатки облачных вычислений и совершить качественный скачок в цифровой трансформации бизнеса.

Договоримся о терминах

Цифровые технологии постоянно обогащают язык новыми терминами, которые описывают новые понятия, концепции, решения или уточняют старые. Недавно на конференциях разгорались споры о значении термина «облачные вычисления», и вот появилась новая тема для дискуссий – Edge Computing.

Термин Edge Computing еще не устоялся, чаще всего под ним понимают концепцию граничных вычислений, в рамках которой ИТ-ресурсы размещаются поближе к конечным устройствам (датчикам, приборам, инструментам), на периферии сети. Информация по максимуму обрабатывается на месте, а в облако передаются уже готовые результаты и отчеты, из облака же на устройства Edge Computing поступают команды, запросы и дополнительная информация. При этом существенно уменьшается нагрузка на каналы связи с дата-центром и снижаются задержки передачи данных, что важно при работе в режиме реального времени. Широкополосные и дорогие каналы связи для быстрой передачи больших объемов информации становятся не нужны.

Еще одним важным преимуществом является автономность. Edge-система может самостоятельно работать при разрывах связи с облаком. Но в отличие от автономных устройств Edge-системы не полностью самостоятельны, их можно сравнить с «облачками», управляемыми из главного облака.

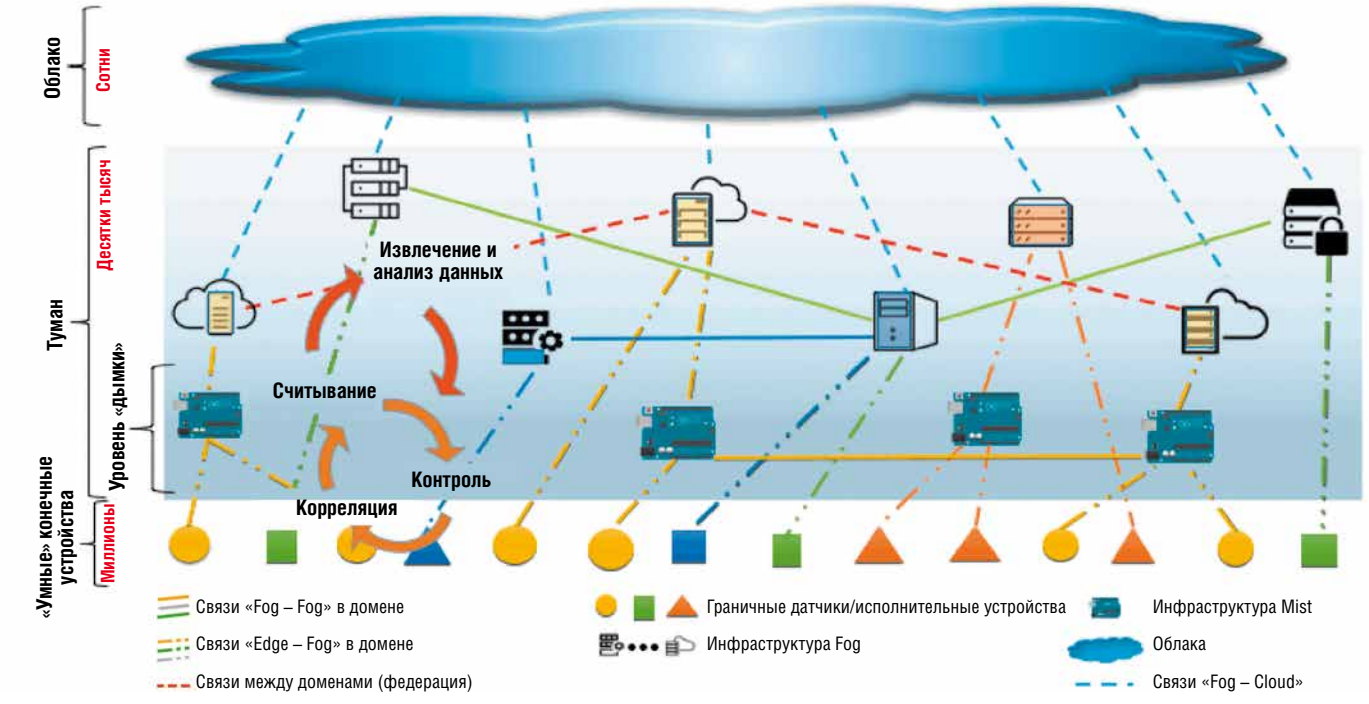
Большинство экспертов уверены в том, что технологии Edge и Cloud Computing будут дополнять друг друга. «С ростом вычислительной мощности и дальнейшей миниатюризацией устройств все больше функций начнет перетекать в Edge Computing, а централизованные облака будут обеспечивать долговременное хранение информации и пользовательский доступ к оперативным и архивным данным», – считает Игорь Гиркин (Cisco).

> Я бы не стал облака и граничные вычисления «сталкивать лбами», сегодня они эффективно дополняют и/или резервируют друг друга, естественно, при условии принятия правильного решения. Облака никуда не денутся и продолжат экспансию на территорию распределенных вычислений и классических ЦОДов, но с меньшими темпами, разделяя рынок с Edge Computing.

Денис Шарапов, менеджер по развитию бизнеса направления «Модульные ЦОДы» подразделения IT Division, Schneider Electric

Тесно связано с Edge Computing понятие Fog Computing. Fog («туман») – это, как и облако, некая связанная распределенная вычислительная мощность, но расположенная «ближе к земле». Некоторые эксперты считают, что Fog и Edge Computing – просто разные маркетинговые термины, описывающие одно и то же. Часто под Fog Computing подразумевают распределенную вычислительную систему расположенных на периферии сети устройств (гиперраспределенное облако), а под Edge Computing – локальную обработку информации датчиков, подключенных к Edge-устройству (мини-ЦОД, бортовой компьютер, персональное вычислительное устройство).

Рис. 1. Экосистема облачных вычислений



Источник: The NIST Definition of Fog Computing, 2017

Схожий подход предлагает и Национальный институт стандартов и технологий США в своем проекте The NIST Definition of Fog Computing, в котором туманные вычисления рассматриваются как модель использования слоя физических или виртуальных ресурсов, находящихся между интеллектуальными конечными устройствами и традиционными облаками или дата-центрами. В документе отмечается, что Fog Computing обеспечивает поддержку вертикально изолированных, чувствительных к задержкам приложений, предоставляя масштабируемые, многоуровневые, централизованные и распределенные системы вычислений, хранения данных и подключений к сети. А Edge Computing определяется как то, что не входит в облако и Fog Computing, – самый край обработки информации, слой сети интернета вещей (рис. 1).

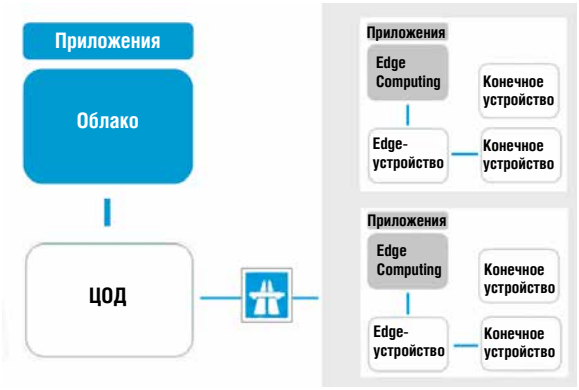
Николай Петров, руководитель отдела вычислительных систем, ГК «ХайТэк»

Если Edge Computing – это миграция вычислений на периферию, ближе к генераторам потоков данных (устройствам, пользователям и т.д.), то Fog Computing представляет собой гиперраспределенное облако, т.е. целый слой вычислительных мощностей разного калибра из их окружения. Не стоит проводить четкую границу между Edge и Fog, поскольку в симбиозе они могут дать огромную выгоду. Например, сбор и первичная обработка данных производятся на Edge-узлах, а анализ, управление и хранение остаются за Fog-слоем.

Рассматривая термины Edge Computing и Fog Computing, нужно принимать во внимание, что они появились как антитеза понятию Cloud Computing, и с этой точки зрения они являются синонимами, указывает И. Гиркин. Он поясняет: «Задачи и Edge, и Fog Computing – перенести обработку данных ближе к источнику их возникновения, особенно в случаях большого потока данных, какой бывает, например, в системах IoT и VR/AR».

Обобщая мнения, можно сказать, что Edge Computing – концепция оптимизации облачных вычислительных систем путем размещения вычислительных ресурсов на границе сети с целью снижения нагрузки на каналы передачи данных и повышения оперативности обработки информации конечных устройств. Составные части, обеспечивающие работу Edge Computing, – каналы связи, физическая и виртуализованная ИТ-инфраструктура и инженерные системы (Edge-устройства, мини- и микроЦОДы), которые создают условия для их функционирования (рис. 2).

Рис. 2. Положение Edge Computing в архитектуре распределенной сети



Edge Computing и телеком

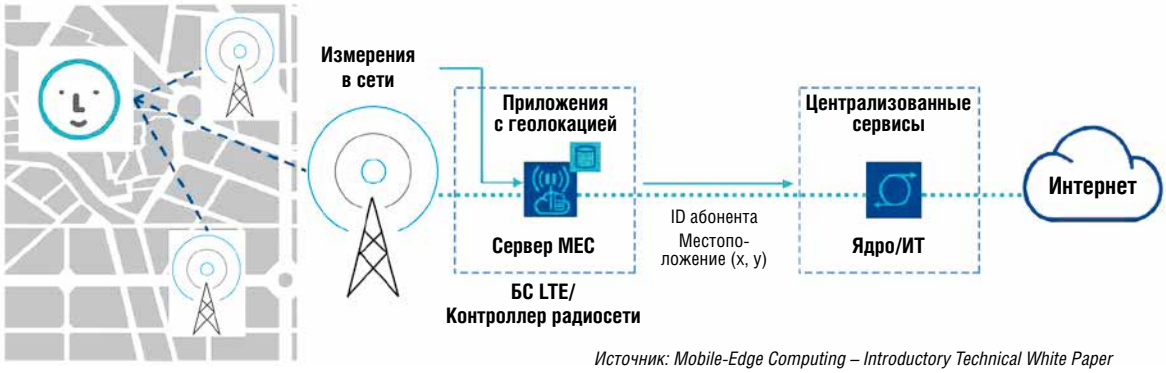
Специалисты в области связи нередко считают, что Edge Computing – понятие из области телекоммуникаций, вспоминая, что именно там появился термин Edge, т.е. связывающий узел на границе сетей, и там же родилась современная концепция Mobile Edge Computing.

В сентябре 2014 г. Европейский институт телекоммуникационных стандартов (ETSI) выпустил предварительный технический документ, посвященный Mobile Edge Computing (MEC). В нем говорится, что MEC обеспечивает возможность выполнения компьютерных и облачных вычислений в радиосети. По сути MEC – это программная платформа для запуска приложений, развернутая на инфраструктуре NFV микроЦОДа, который вынесен в радиосеть, например на базовую станцию. Таким образом операторы мобильной связи могут выступить в роли провайдеров услуг периферийных вычислений.

MEC позволяет операторам сотовой связи открывать свою сеть радиодоступа уполномоченным третьим сторонам, таким как разработчики приложений и поставщики контента. Для них MEC предоставляет стандартизированную открытую среду с максимальной пропускной способностью, минимальными задержками и доступом в реальном времени к оперативной информации – текущим параметрам работы сети, местонахождению абонента и т.д. (рис. 3).

Сергей Безрученко, директор по продажам, Brain4Net

Рост объемов трафика предъявит новые требования к сетям операторов, которые будут вынуждены трансформировать централизованное ядро мобильной сети (IMS Core) в распределенные сущности. Это необходимо, чтобы снизить нагрузку на ядро сети и уменьшить объем трафика, проходящего через сеть оператора.



Источник: Mobile-Edge Computing – Introductory Technical White Paper

Рис. 3. Определение положения абонента сотовой сети на месте с помощью MEC

Недавно группа ETSI, занимающаяся MEC, расширила сферу своей деятельности, включив в нее помимо сотовой связи другие технологии доступа, и ввела термин Multi-Access Edge Computing.

Используя архитектуру Multi-Access Edge Computing, операторы связи получают возможность разворачивать на границе сети приложения нового поколения, в том числе CDN, DNS, 5G и телеметрические сервисы IoT, шейпинг мобильного трафика. Они смогут предлагать геолокационные сервисы, видеоаналитику, услуги дополненной реальности и информацию для подключенных автомобилей. Более того, у операторов будет возможность предоставлять инфраструктуру по сервисной модели сторонним организациям. Это важно в первую очередь для предприятий среднего и малого бизнеса, которым открывается доступ к современным технологиям.

Multi-Access Edge Computing, по мнению Артема Гениева (VMware), идеально подходит для того, чтобы обеспечить готовность имеющейся инфраструктуры для развертывания услуг высокой пропускной способности с ультранизкими задержками и в будущем плавно перейти к сетям 5G. «За счет предоставления на границе сети услуг облачных вычислений, которые работают в режиме, близком к реальному времени, Multi-Access Edge Computing открывает приложениям мгновенный доступ к информации в сети, улучшая пользовательский опыт и создавая дополнительные возможности для инноваций», – говорит он.

Edge Computing в рамках закона

Отечественное законодательство, предписывающее хранить персональные данные россиян на территории страны, не до конца понятные последствия принятия «пакета Яровой» и закона о безопасности критической информационной инфраструктуры заставляют глобальные компании задуматься о необходимости обеспечивать хранение большого количества данных на территории России.

По сути, вычислительные мощности выносятся из глобальной системы на периферию при сохранении возможности взаимодействия с центром и интегрированной обработки информации. Такого рода решения некоторые эксперты рассматривают тоже как Edge Computing, хотя дело часто сводится к простой репликации локальных данных в ЦОД зарубежной компании, где и проводится окончательная обработка.

Свойства MEC

Характеристика	Обеспечиваемые возможности
Автономность	Не зависящая от остальной части сети работа при наличии доступа к локальным ресурсам. Это особенно важно для сценариев межмашинного взаимодействия, когда для обмена не используется центральное облако, и в условиях нестабильной связи
Близость к датчикам	Оперативная обработка поступающей информации и совершение управляющих воздействий без использования вычислительных мощностей центра. В центр отправляется агрегированная информация для аналитических отчетов и обработки в системах Machine Learning и Big Data
Малая задержка	Минимизация времени передачи информации благодаря тому, что вычислительные мощности находятся рядом с объектом
Фиксированное расположение вычислительного узла	Повышение точности определения положения подключенных мобильных устройств, что важно при предоставлении услуг, основанных на анализе передвижений объекта (например, посылка рекламных сообщений магазина, находящегося рядом с клиентом)
Оперативная информация о состоянии сети	Обработка в режиме реального времени информации об условиях радиосвязи и сетевой статистики

У российских заказчиков время от времени возникают задачи, для которых необходимы решения класса Edge Computing, но это скорее исключение, чем правило. Мы видим большой интерес со стороны заказчиков с зарубежными представительствами или географически удаленными локациями, которым необходимы высокозащищенные локальные вычислительные ресурсы на уровне филиалов с моментальной репликацией данных в ЦОД или облако.

Александр Стулов, глава представительства в России и СНГ, Riverbed Technology

Игорь Гиркин, менеджер по продвижению новых технологий, Cisco

В подходе Edge Computing нет ничего нового: на подобном принципе обработки информации основаны АСУ ТП, где роль узла Edge Computing исполняет программируемый логический контроллер, а источником данных является управляемое контроллером оконечное устройство (привод, робот, манометр, задвижка и т.д.). Но важно, что Edge Computing дополняет традиционный подход АСУ ТП возможностью получения данных от нескольких систем управления с целью анализа взаимной корреляции событий и обработки данных на краю сети, ближе к источникам информации.

Тем не менее на рынке есть решения, где и обработка выполняется в облаке локального ЦОДа. Так происходит, например, в Microsoft Azure Stack или в решении компании Oracle, когда весь функционал, доступный в облаке Oracle, переносится в дата-центр заказчика на программно-аппаратный комплекс Oracle Cloud Machine. Использование в локальном ЦОДе и публичном облаке Oracle Cloud одного и того же программного обеспечения позволяет переносить между ними приложения и данные со скоростью миграции, а размещение данных в ЦОДе клиента минимизирует задержки в сети.

Рис. 4. Всепогодный промышленный компьютер МС-720 «Дозор» используется в системе контроля ПДД

В России обсуждаются изменения в законодательстве об информации, которые позволят принять закон о хранении на территории страны технологических данных, несущих угрозы энергетической безопасности (по аналогии с поправками в закон «О персональных данных»). По сути, речь идет о локализации хранения данных индустриального интернета вещей. Новое законодательство выступит еще одним катализатором развития ЦОДов в стране.

Таким образом, основные точки роста Edge Computing в России – это предприятия с ограничениями на передачу данных в облако, желающие внедрять решения IoT и машинное обучение, а также имеющие объекты с нестабильным подключением к интернету. В нашей стране с большим трудом продвигаются полностью облачные технологии, поэтому, по мнению экспертов московского офиса Microsoft, такой гибридный подход очень перспективен.

Облака, Edge Computing и миры Джеймса Кэмерона

Постапокалиптический мир фильмов Джеймса Кэмерона – общество после катастрофы, вызванной искусственным интеллектом. Операторы в спешке пытаются отключить «Скайнет» – неожиданно обретшую сознание боевую информационно-управляющую систему министерства обороны США. В качестве самозащиты суперкомпьютер стремится уничтожить человечество и развязывает ядерную войну. Для борьбы с выжившим после катастрофы населением «Скайнет» создает автономные, принимающие по ситуации решения устройства – терминаторов. Переведя на современный ИТ-язык: действующая в облаке на базе технологий Machine Learning и AI критическая информационная компьютерная система выходит из-под контроля персонала, начинает борьбу с угрожающим ее существованию человечеством и создает Edge-устройства, использующие Edge Computing для окончательного решения вопроса.

Фантастика – попытка заглянуть в будущее, опираясь на прошлое и настоящее. Индустрия 4.0 и процессы цифровой трансформации стремительно увеличивают нагрузку на сеть. Аналитики утверждают, что к 2020 г. число подключенных к интернету устройств достигнет 50 млрд. Число «нечеловеческих» пользователей намного превысит число людей, и они будут генерировать огромные объемы информации, которую надо анализировать, причем зачастую почти мгновенно... Терминатор не может для принятия каждого решения обращаться за подсказкой в «Скайнет». Оперативная информация должна обрабатываться локально и быстро. Искусствен-

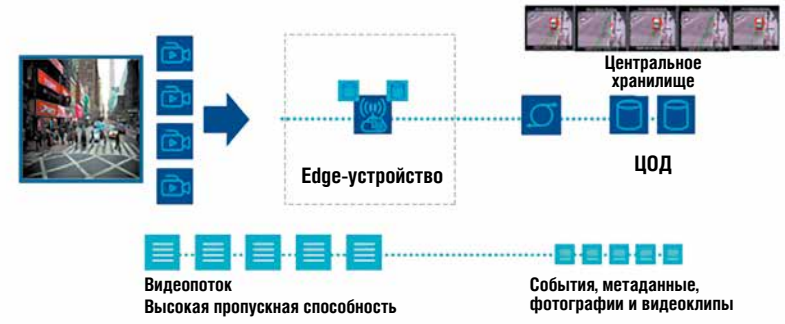
ный интеллект переносит часть своей вычислительной нагрузки на границу сети, на уровень армии созданных им роботов-убийц.

Edge Computing и IoT

Неоднозначность термина Edge Computing не мешает аналитикам высоко оценивать перспективы концепции граничных вычислений. Так, Gartner считает Edge Computing одним из десяти основных трендов развития технологий в 2018 г. Эта концепция, впервые появившаяся на кривой зрелости технологий Gartner в 2017 г., уже подходит к вершине хайпа. Стоит отметить, что многие другие перспективные технологии – виртуальная реальность, 5G, платформы IoT, автономные автомобили, «умные» роботы, «умный» дом, – которые находятся вблизи пика завышенных ожиданий или выходят на плато продуктивности, будут оказывать сильное влияние на развитие рынка Edge Computing. В IDC считают, что к 2020 г. расходы на граничную ИТ-инфраструктуру достигнут 18% общей суммы расходов на инфраструктуру IoT. А согласно прогнозу MarketsandMarkets, рынок Edge Computing к 2022 г. достигнет $6,72 млрд.

Одним из главных катализаторов развития рынка граничных вычислений станет массовое использование технологий интернета вещей. Концепция Edge Computing будет активно внедряться на транспорте, в промышленности и даже в финансовой сфере, например при создании «умных» банкоматов, которые не только выдают деньги, но и анализируют видеопоток с камер наблюдения, распознают лица потенциальных мошенников, блокируют выдачу им наличных или даже анализируют криминогенную ситуацию рядом с устройством и посылают сигнал тревоги службе безопасности.

Развитие российского рынка граничных вычислений отстает от мирового, но отечественные разработки существуют. Скажем, ультразащищенный всепогодный промышленный компьютер МС-720 «Дозор» уже работает на дорогах столицы (рис. 4, 5). Четырехъядерный процессор обрабатывает в реальном времени видеопоток от восьми (четыре в одну сторону и четыре в другую) камер наблюдения. Система выявляет нарушения ПДД, распознает номер автомобиля и посылает в центр управления дорожным движением Москвы информацию, включающую фотографии момента нарушения. «Письмо счастья» направляется водителю по обычной и электронной почте. Через интернет нарушитель может оперативно оплатить штраф. Все происходит в автоматическом режиме, быстро и эффективно. Многие читатели наверняка проверили работу этой системы на себе. Устройство рассчитано на непрерывную работу без обслуживания в течение пяти лет, при нарушениях в электропитании перезагружается автоматически, в случае замерзания предварительно прогревается. Видео архивируется, чтобы можно было восстановить картину за заданный интервал времени. Компьютер размещается в антивандальном шкафу, кабели защищаются металлическими рукавами.



▲ **Рис. 5. Обработка получаемых с видеокамер видеопотоков с использованием Edge-устройств**

Говорить о том, что рынок Edge Computing сформировался, еще рано – хотя бы потому, что аппаратная составляющая достигла подходящего уровня технологического совершенства не так давно, буквально три-четыре года назад. До этого датчики, коммутаторы Ethernet, Wi-Fi-роутеры и прочие девайсы были заняты своими прямыми

МНЕНИЕ ЭКСПЕРТА

От специализированных решений к типовым

В ближайшие пять лет рынок будет активно формироваться, и мы увидим готовые решения, ориентированные на различные сферы бизнеса, телеком, производство и т.д.

В отличие от европейского на российском рынке решений Edge Computing нет стандартов, которых нужно придерживаться. Производитель старается создать максимально стандартизированное законченное решение, заказчики же предъявляют все новые и новые требования, возможно, не совсем аргументированные, которые приводят к необходимости изменения стандартных решений.

В этом есть свои плюсы и минусы. Стандартное решение будет проверено и оттестировано производителем на заводе, собрано максимально качественно и надежно. Специализированные решения требуют особого подхода и дополнительных трудозатрат как от заказчика, так и от производителя. Однако именно сложные и интересные задачи ложатся в основу следующих стандартных решений, задают тренд на будущее, заставляя производителей вкладываться в разработки.

Александр Нилов, старший менеджер по продукции для ИТ-инфраструктуры, Rittal

«обязанностями» – фиксировали параметры и/или передавали данные. Возможностей бортовой логики хватало только на это, не более. «Со снижением стоимости флеш-памяти и повышением производительности процессоров появилось доступное "железо", на котором можно размещать виртуальные машины – достаточно сложные для того, чтобы на их основе реализовывать функциональность Edge Computing», – комментирует ситуацию Сергей Монин (Softline).

Леонид Юль, ведущий пресейл-инженер, C3 Solutions

Миграция данных в облако – свершившийся факт. Но он выявил проблемные зоны: узость каналов, длительное время реакции. Edge Computing – это ответ для тех, кто хочет получить преимущества облака без его недостатков: быстрая обработка локальных данных и при необходимости – использование облачных мощностей для централизации.

В качестве примера объекта, на котором востребованы технологии Edge Computing, С. Монин приводит транспортный трубопровод, где нужно быстро распознать утечку и дать сигнал перекрыть трубу и где нет времени ждать отправки сигнала через спутник, поскольку экономический, экологический и репутационный ущерб от каждой секунды промедления будет значительным. Другие примеры – опасные производства, а также индустрия космических запусков, где счет идет на миллисекунды и скорость реакции исполнительных систем на изменившиеся условия имеет решающее значение.

Делясь опытом внедрения Edge Computing, эксперт Softline описывает проект, реализованный для сети ресторанов быстрого питания: «Там уже была развернута инфраструктура датчиков, информация с которых собиралась через коммутаторы (по одному на каждый ресторан) и отправлялась в облако Microsoft Azure, где и обрабатывалась. Мы добавили в коммутаторы возможность анализировать показания с помощью имеющихся у них «на борту» ресурсов. Это необходимо, чтобы немедленно реагировать на всевозможные нештатные ситуации, например на повышение температуры в критических зонах горячего цеха. В данном случае на телефон менеджера отправляется SMS-сообщение, которое служит сигналом принять меры. Это изменение инфраструктуры сделано для подстраховки – если связи с облаком в критический момент не будет».

Денис Сереченко, директор по развитию бизнеса в России, Huawei Enterprise Business Group

Рынок Edge Computing в привычном его понимании пока не сформировался даже в США. Что уж говорить о российском ИТ-рынке, который традиционно отстает от американского лет на пять. В России все еще ощущается нехватка ИТ-инфраструктуры и потребность в типовых решениях. Edge Computing – это следующий шаг на пути технологического развития, который призван оптимизировать существующие ресурсы.

Компания «ХайТэк» использовала технологии Edge Computing при создании системы автоматического контроля качества на линиях сборки изделий для крупного наукоемкого предприятия. Механизм следующий: умные инструменты, такие как штангенциркули, динамометрические ключи и др., передают по Wi-Fi все данные о сборке изделия в специальный компьютер, находящийся в цехе, который в свою очередь совершает ряд вычислений и проверяет, правильно ли собрано изделие, соответствует ли ГОСТам и т.д. Далее Edge Computing начинает взаимодействовать с Cloud Computing: на основе вычислений цехового компьютера формируется отчет, поступающий в PLM-систему, которая отслеживает жизненный цикл изделия. «Реализованное решение позволило предприятию обеспечить максимально безопасную и надежную сборку продукции и, как следствие, минимизировать репутационные риски, связанные с человеческим фактором», – подчеркивает Николай Петров из «ХайТэк».

Помимо производств с высоким уровнем автоматизации и территориально распределенных компаний с узкими каналами связи между офисами в качестве интересантов Edge Computing Леонид Юль (C3 Solutions) выделяет торговые сети. Более того, именно торговые сети, по его мнению, являются пионерами на российском рынке Edge Computing. «Высокая оборачиваемость и малые сроки хранения продукции, необходимость проактивной работы с потребителями позволяют быстро ощутить пользу от внедрения этой технологии», – отмечает Л. Юль.

Архитектура и сценарии

Один вариант распределения вычислительной нагрузки между центром и периферийными устройствами – полностью централизованная система сбора данных и управления, например, подключение всех датчиков и устройств напрямую к расположенной в публичном облаке платформе интернета вещей. Другой крайний случай – станок с ЦПУ, автономно работающий по заданной программе. Edge Computing занимает

между двумя сценариями промежуточное положение, что усложняет использование этой технологии. Нужно найти баланс между централизацией и децентрализацией, обеспечить оркестрацию работы вынесенных на границу сети вычислительных систем, что сделать совсем не просто. Кроме того, часто нужна гибкость в изменении архитектуры, которую могут обеспечить программно определяемая инфраструктура и контейнеризация.

В список ключевых технологий, дополняющих серверную виртуализацию для полноценной реализации Edge-облака, по мнению А. Гениева из VMware, входят: программно определяемое хранение данных, программно определяемые сети, а также средства автоматизированного развертывания и управления жизненным циклом аппаратных и программных компонентов Edge-облака. Они позволяют реализовать полный функционал облака корпоративного класса в максимально компактном формфакторе, что делает возможным быстрое развертывание Edge-облака в нетрадиционном для ЦОДа окружении (например, на локомотиве или фабрике). «Средства автоматизации упрощают развертывание Edge-облака и позволяют снизить требования к компетенции персонала, что особенно ценно при размещении Edge-облаков на множестве объектов инфраструктуры предприятия», – поясняет А. Гениев.

Классический вариант архитектуры распределенной сети с использованием Edge Computing: **ЦОД – мини-ЦОД – конечные устройства**, где мини-ЦОД имеет инженерную инфраструктуру, необходимую для размещения и работы активного ИТ-оборудования: стойки, системы холодоснабжения, бесперебойного питания, пожаротушения, мониторинга и токораспределения. Примером может служить контейнерный ЦОД в тайге, обеспечивающий обработку информации, которая поступает с устройств, связанных с добычей нефти. В качестве граничного дата-центра может выступать и микроЦОД – шкаф с инфраструктурой для размещения вычислительных мощностей.

«Для того чтобы концепция Edge Computing работала, нужны локальные распределенные вычислительные узлы – полностью дистанционно управляемые микро- или мини-ЦОДы с развитой инженерной инфраструктурой, где стояли бы несколько серверов с «выносами» локальной обработки и управления. Такие решения в России продаются, но в единичных экземплярах, хотя в странах с развитой цифровой экономикой подобные комплексы разлетаются как горячие пирожки», – отмечает С. Белик из «Телекор».

Некоторые специалисты идут дальше и рассматривают в качестве Edge-устройств любые вычислительные устройства, способные собирать и обрабатывать информацию с датчиков, в том числе персональные компьютеры и смартфоны. Носимые человеком гаджеты могут анализировать данные с видеокамер, микрофонов, подключаемых внешних устройств, скажем, таких, которые позволяют самостоятельно сделать УЗИ исследуемых органов, посмотреть картинку на экране смартфона и послать врачу. Нейросеть, разработанная стартапом Cardiogram, способна по характеру пульса человека диагностировать диабет с точностью 85%. При этом для использования не нужны специальные медицинские приборы – достаточно умных часов или другого носимого устройства.

Edge Computing и виртуальная реальность

Трудно представить внедрение технологий виртуальной реальности без использования Edge Computing, ведь для создания быстро изменяющихся картин виртуального мира надо обрабатывать огромные объемы информации. Поми-

МНЕНИЕ ЭКСПЕРТА

Edge Computing – это децентрализованное управление и централизованный контроль

Edge Computing – не просто вычисления в распределенных вычислительных узлах. Эта концепция подразумевает выполнение в распределенных узлах изменяющейся части вычислений одной и той же прикладной задачи (или отдельных функциональных блоков) и «досчет» задачи в централизованных, больших по масштабу узлах с обратной связью.

Технически реализовать такие распределенные вычисления сложнее, чем просто grid-систему, поскольку прикладное ПО и слой middleware помимо вычислений в сети узлов должны определять правила взаимодействия центрального блока и удаленных блоков вычислений, в идеале автоматически перераспределять нагрузку и доли обработки между центром и удаленными узлами, обновлять правила взаимодействия и т.д.

Обеспечить согласованную работу системы с большим количеством связей сложно. Но игра стоит свеч, да и в ситуации, когда объем данных увеличивается на порядки, другого выхода просто нет. Edge Computing – это естественная реализация одного из ключевых принципов построения эффективных систем управления – «децентрализованное управление и централизованный контроль».

Сергей Белик, заместитель генерального директора по развитию, «Телекор»

Сергей Монин, эксперт в области решений по промышленному интернету вещей, ГК Softline

На сегодняшнем уровне развития граничные вычисления будут востребованы везде, где большие расстояния и нестабильность сетевого соединения между исполнительными механизмами и центром принятия решений являются критическими факторами. Мгновенная реакция на изменение обстановки – сильная сторона Edge Computing.

мо индустрии игр, технологии VR могут быть востребованы в архитектуре и дизайне, в обучении, спорте, искусстве и медицине и даже в секс-индустрии. В вышедшем в этом году сериале «Видоизмененный углерод» виртуальная реальность успешно использовалась для проведения изощренных бесконтактных пыток. Так что для терминатора и воюющей с человечеством системы «Скайнет» технология тоже может быть интересна.

Еще одна технология, которая, по мнению Павла Рыцева из ALP Group, повлияет на рынок Edge Computing, когда задержка между действием пользователя и ответом системы станет минимальной, – это стриминг игр. Схема здесь понятна: у пользователя есть терминал, показывающий и принимающий «картинку», а в ЦОДе стоят серверы с массой видеокарт, которые и обрабатывают изображение.

Edge Computing и распределенные базы данных

Как правило, устройство Edge Computing – это полноценная вычислительная система, включающая системы хранения данных. Таковой может быть и классическая СХД, и программно определяемое хранилище, и просто жесткий диск. В любом случае появляются возможности для построения на этих устройствах распределенных баз данных, что особенно привлекательно для организации резервирования при наличии горизонтальных связей между Edge-ЦОДами. Однако если каналы передачи данных в решении Edge Computing слабо защищены от несанкционированного доступа, то нужно строить серьезные системы безопасности или принимать возрастающие риски, предупреждает С. Белик («Телекор»).

И здесь может помочь технология блокчейн. «Edge Computing и блокчейн как нельзя лучше дополняют друг друга, – считает С. Белик. – Блокчейн обеспечивает защищенную, не подверженную модификации передачу данных по любым каналам, а Edge Computing – множество распределенных вычислительных узлов для верификации тех самых цепочек блоков». Ценная информация может не передаваться в центр, а записываться в распределенные реестры. В этом случае Edge-узлы могут выступать как ноды блокчейн-цепи поставщиков и потребителей информации, а записанная в блоках информация становится «общей версией правды». Интересным представляется использование криптовалют, которые позволят без посредников провести взаимные расчеты между устройствами интернета вещей. Работы в этом направлении уже ведутся.

В прошлом году энергетическая компания RWE открыла в Германии 100 автономных зарядных станций для электромобилей, работающих на базе блокчейна Ethereum. Приложение на смартфоне под названием Share & Charge и смарт-контракты на блокчейне Ethereum, интегрированные в зарядные станции, дадут возможность пользователям без участия третьей

МНЕНИЕ ЭКСПЕРТА

Неочевидные, но вероятные ошибки: как избежать

Денис Тукалевский, независимый эксперт

В большинстве случаев децентрализация ЦОДа решает прикладную задачу оптимизации бизнес-услуги или снижения операционных расходов на инфраструктуру. Основная цель в таких случаях – уменьшение сетевого трафика и/или времени обработки клиентского запроса. Как правило, нагрузка перераспределяется с основного ЦОДа на вычислительные/сетевые мощности, расположенные максимально близко к конечному пользователю бизнес- или ИТ-услуг. Для подобных случаев создают микроЦОДы – небольшие серверные помещения, с обособленной инфраструктурой и вычислительной мощностью. Избежать ошибок, сэкономить время и ресурсы при развертывании микроЦОДов помогут советы из практики.

1. Применяйте комплексный подход. В проекте микроЦОДа должны быть увязаны в единое целое строительная подготовка, инженерная и сетевая инфраструктура, вычислительные мощности, а также учтены ширина каналов и уровень резервирования конечного решения. Как правило, в крупных корпорациях задача оптимизации делегируется подразделению, которое имеет компетенции только в одном из направлений. Соответственно, детально прорабатывается только часть решения, возникают перекосы в реализации, которые могут привести к остановке ЦОДа и прекращению предоставления услуг. Чаще всего ошибаются в расчете ширины каналов передачи данных, мощности систем холо-

стороны предоплачивать услуги, заряжать электромобиль, возвращать свой депозит, наблюдать за процессом зарядки в реальном времени, контролировать затраты и отслеживать ближайшие заправки. В перспективе автомобили с цифровыми бумажниками смогут «говорить» с автономными электрическими зарядными станциями, оплачивая зарядку в автоматическом режиме.

Мобильные Edge-ЦОДы

Часто требуется, чтобы периферийные вычислительные узлы не находились на одном месте, а перемещались вместе с устройствами сбора и обработки информации. Это накладывает дополнительные требования на инфраструктуру мини-ЦОДа, который помимо всего должен теперь работать в условиях вибрации. Полноценный мобильный ЦОД, удовлетворяющий высоким требованиям по внешним воздействиям, поддержанию температурных режимов, системам резервирования электропитания, будет по карману разве что военным. С другой стороны, в качестве микроЦОДов для Edge Computing можно рассматривать вычислительные системы современных локомотивов и «умных» автомобилей, когда они являются частью распределенной сети компании, обрабатывающей информацию и координирующей действия своих автономных узлов. Примером такой системы может служить созданная на платформе Predix система индустриального интернета, объединяющая 21 тыс. локомотивов компании GE.

Самоуправляемые автомобили, создаваемые компаниями Tesla Motors и «Яндекс», пока работают достаточно автономно. В сети 5G они смогут в режиме реального времени обмениваться информацией с Edge-облаком, в котором будет постоянно находиться и обновляться информация о дорожной ситуации и климатических условиях на пути следования. Оперативное взаимодействие между Edge-устройствами позволит избежать такой аварии, которая произошла, когда бортовой компьютер автомобиля Tesla принял разворачивающийся поперек дороги грузовик за рекламный плакат над дорогой.

Одна крупная европейская транспортная компания, как рассказал А. Гениев, стремясь снизить издержки и повысить эффективность перевозок, оснастила Edge-облаками локомотивы своих поездов. Требовалось в реальном времени анализировать информацию, поступающую от систем поезда, – метрики работы двигателя, данные о трафике, погодных условиях и т.д., – для обеспечения эффективной и бесперебойной работы, а также для оптимизации маршрута движения состава. Решение было найдено в использовании микроЦОДов, состоящих из виртуализированных блейд-серверов и программно определяемого хранилища. Такой микроЦОД имеет сверхкомпактное исполнение, но при этом обладает выдающимися характеристиками производительности и надежности, позволяя анализировать события и реагировать на них в реальном времени.

Посмотрите на карту нашей страны. Пересчитайте расстояния в задержку сигнала, оцените, насколько страна покрыта каналами передачи данных. В России огромный потенциал использования Edge Computing. Вопрос в финансировании этого спроса.

Валентин Фосс, директор по маркетингу и сбыту, «Утилекс»

МНЕНИЕ ЭКСПЕРТА

доснабжения и бесперебойного электропитания; забывают про резервирование и время автономии ЦОДа. Для исключения подобных ошибок рекомендуется создавать полноценную проектную команду с привлечением специалистов всех направлений. При отсутствии собственных компетенций лучше привлечь внешних специалистов.

2. Используйте типовые решения. Как показала практика, самая затратная статья для сети распределенных микроЦОДов – эксплуатация. Причина проста: в разных локальных проектах устанавливается разное оборудование. Причем часть оборудования поставляется централизованно, часть выбирается локально, по месту размещения ЦОДа. Казалось бы, эксплуатация оборудования, широко применяемого в регионе, должна быть дешевле и проще. На деле ситуация выглядит по-другому: уровень обслуживания оставляет желать лучшего, а с запчастями постоянные перебои. При сроке жизни ЦОДа свыше трех-четырех лет, даже с учетом накладных расходов на централизованный склад и доставку запчастей в регионы, эксплуатация типовых решений обходится на 15–20% дешевле.

3. Пишите подробные инструкции. После запуска проекта поддержку существующего решения зачастую осуществляют локальные специалисты, в нагрузку к уже имеющимся функциональным обязанностям. Это, безусловно, сокращает расходы на персонал, но обратной стороной является отсутствие компетенции и необходимых навыков для обеспечения поддержки. Решением может послужить создание подробных инструкций по обслуживанию и эксплуатации оборудования, базы знаний по типовым проблемам и способам их устранения.

Артем Гениев,
архитектор бизнес-решений, VMware

Edge Computing – первая точка в долгосрочном тренде перехода от максимально централизованных систем к максимально децентрализованным, так называемым Fog Computing. Основными драйверами развития Edge Computing станут различные сценарии IoT и переход на сети 5G.

Edge Computing и AI

Важное преимущество технологии Edge Computing – возможность работы в условиях плохой связи с дата-центром. Постоянный канал не важен, главное найти возможность послать в Edge-устройство запрос и при появившейся возможности получить от него отчет. Можно повысить эффективность автономной работы, используя нейронные сети, системы машинного обучения и искусственный интеллект. Например, центральное облако обучает свою нейронную сеть, а полученную модель загружает в нейронные сети устройств, выполняющих граничные вычисления.

Мобильность Edge-устройств создает новые возможности для силовых структур. Искусственный интеллект позволяет, скажем, дронам стартапа Exyn Technologies летать автономно даже в темноте, внутри помещений и без GPS, ориентируясь при помощи сенсоров и прокладывая маршрут по ходу движения. Ролик активистов за запрет автономного оружия, в котором маленькие дроны с взрывчаткой находили и убивали преступников, распознавая лица по фотографиям из социальных сетей, стал хитом интернета в январе нынешнего года. А в феврале в прессе появились сообщения о реальном китайском проекте использования технологий AI на атомных подводных лодках. Пока искусственный интеллект будет только подсказывать командирам субмарин – окончательное решение остается за человеком. Но «мир терминатора» явно становится ближе.

Прекрасное далеко

... Свободная воля терминаторов воспринималась «Скайнет» как угроза, как возможность выступления против своего создателя. Представляет ли Edge Computing угрозу для облачных вычислений, классического Cloud Computing, до конца не понятно. В последнем сезоне сериала «Черное зеркало» мы видели постапокалиптический мир – мир победивших локальных вычислений. Человечество добивают полностью автономные, видимо, созданные для охраны роботы-псы, которым никакое центральное облако уже не нужно.

Надеемся, этого не произойдет. В соответствии с законами диалектики развитие идет по спирали. Персональные компьютеры пришли на смену мейнфреймам, потом технологии опять качнулись в сторону централизации, и мейнстримом стали облака. При этом и мейнфреймы, и персональные компьютеры никуда не делись, просто заняли свои рыночные ниши. Новый виток ведет к распределенным вычислениям и переносу вычислительных мощностей на границы сети. Edge Computing не победит Cloud, а просто его дополнит, используя имеющиеся у технологии преимущества. ИКС

МНЕНИЕ ЭКСПЕРТА

Больше интеллекта – к границе сети

Дермот О'Коннел,
вице-президент и руководитель подразделения OEM- и IoT-решений в регионе EMEA, Dell EMC

Граничные вычисления в ближайшие несколько лет станут обычным явлением в отраслях, использующих для предоставления услуг автоматическую обработку информации в режиме реального времени. Возьмем, к примеру, здравоохранение. Уже начинают внедряться активные и интеллектуальные средства мониторинга работы сердца, а ожидание ответа от централизованной облачной инфраструктуры, даже если она находится «в нескольких секундах», может стоить пациенту жизни.

Для поддержки граничных вычислений потребуется современная ИТ-инфраструктура, причем нередко в местах, неподходящих для установки стандартного сервера. Так, нефтегазовым компаниям часто необходимо разворачивать ИТ-системы в районах с суровыми условиями, например в море, или в ограниченном пространстве. Такие отрасли, как оборона, сталкиваются с аналогичными проблемами, поскольку создание усиленной защиты, основанной на анализе данных «на границе», в случае важных событий требует крайне быстрой обработки информации.

Производственные отрасли уже перестраиваются, используя граничные вычисления. Мы находимся на пороге четвертой промышленной революции, которая должна ускорить производственные процессы в течение следующих пяти лет благодаря таким новым технологиям, как робототехника, 3D-печать и интернет вещей. Рутинные операции будут выполнять роботы, «производства без границ» станут мейнстримом, беспрецедентным образом будут автоматизированы цепочки поставок. Внедрению таких новшеств, особенно это касается производственных площадок в удаленных местностях, будут способствовать граничные вычисления в сочетании с современной, защищенной ИТ-инфраструктурой.

Промышленные ИБП для дата-центров

Высоконадежные решения для промышленности могут быть конкурентоспособными на рынке систем гарантированного электроснабжения ЦОДов, считает генеральный директор компании «Абсолютные Технологии» Олег Четвергов.

Олег Четвергов

– Наша компания 20 лет успешно работает на российском рынке высококачественного оборудования для систем гарантированного и бесперебойного электроснабжения. За это время накопился огромный опыт взаимодействия с компанией GE, который использовался при налаживании производства ИБП «Абитех», открывшегося в начале года в Долгопрудном.

Локализация ИБП GE началась с трансформаторных машин. Трансформаторные ИБП – это решение, обеспечивающее надежность и безопасность промышленного уровня при нестабильном входном электропитании. При этом ИБП «Абитех» имеют меньшие массогабаритные показатели по сравнению с присутствующими на российском рынке промышленными ИБП.

Часто ИБП субъективно относят к тому или иному классу исходя из наличия трансформатора. Если трансформатор имеется, то это устройство для промышленности, если нет – для ИТ. Но определение надежности системы бесперебойного питания в промышленности и в ИТ одно и то же. Наша компания обеспечивает максимальный уровень надежности системы и выпускает трансформаторные аппараты и для промышленности, и для ЦОДов.

Мы объясняем заказчику плюсы и минусы предлагаемых решений. Например, бестрансформаторные машины дешевле и легче. Но если для заказчика важнее безопасность и надежность, то лучше остановиться на трансформаторном решении. Для снижения массогабаритных показателей системы в целом мы располагаем типовым решением с применением литий-ионных АКБ. С точки зрения надежности трансформаторный ИБП – как автомат Калашникова, он прост и безотказен. А если рассматривать не только начальную цену, но и стоимость владения, то через пять лет затраты на решения будут сопоставимы.

Аппараты обслуживаются и ремонтируются непосредственно на объекте. Сервис – одно из наших наиболее сильных конкурентных преимуществ. Работа с компанией GE приучила, что ни один аппарат не должен остаться без поддержки. У нас большой склад ЗИП для молниеносного реагирования на запросы, что очень позитивно воспринимается заказчиками.

– Какие еще конкурентные преимущества стоит отметить?

– В ИБП «Абитех» используется элементная база GE, одного из ведущих мировых поставщиков ИБП. Это выгодное отличие от многих других производителей, в том числе из Китая.

При этом компания способна оказывать достойную конкуренцию по цене старому пулу европейских производителей. В тендерах по выбору оборудования при подведении итогов допускается, чтобы отечественный аналог был на 15% дороже импортного. За счет этого наша продукция будет успешно конкурировать по цене с аналогичными ИБП, собранными на заводах Европы.

Компания «Абсолютные Технологии» предоставляет весь комплекс услуг сопровождения ИБП у заказчиков, а также обучает инженеров партнерских компаний в своем учебном центре – это еще одна наша сильная сторона. Мы ежемесячно проводим тренинг с выдачей сертификатов инженерам партнеров, которые могут зарабатывать деньги на запуске аппаратов. Наличие большого количества обученных специалистов по всей России, в Белоруссии, Казахстане и Узбекистане – тоже конкурентное преимущество.

– Почему компания «Абсолютные Технологии», хорошо известная как интегратор электротехнического оборудования, решила заняться производством? Какие проблемы локализации были при этом выявлены?

– Государство поставило задачу – производить отечественный продукт. Развертывание производства ИБП «Абитех» – ответ на новые требования времени. Однако замена узлов в импортных решениях повышает цену: по нашим оценкам, собранный на 60% из российских комплектующих ИБП будет в 2,5 раза дороже. Такое изделие нельзя продать, оно не будет востребовано рынком. Другой момент – при таком подходе страдает качество.

Продукция GE – это результат успешной работы над многими поколениями устройств, тщательной проработки всех комплектующих. Механическая замена деталей на российские аналоги может сказаться на надежности аппарата, да и устраивающие по качеству комплектующие найти в стране нелегко. Так что в ближайшей перспективе задача полного импортозамещения не стоит. Но все, что касается сборки, параметрирования и выходного тестирования, компания взяла на себя. Работы проводятся силами наших специалистов, прошедших обучение на заводе GE.

Другие проблемы локализации: сложности поиска площадки, удовлетворяющей высоким требованиям нормативов GE, и трудности организации взаимодействия с поставщиками.

– Поделитесь планами дальнейшего развития производства.

– Будем расширять линейку ИБП «Абитех», чтобы конкурировать на рынке в более широком сегменте и ценовом диапазоне. Кроме того, на той же площадке в Долгопрудном уже начались работы по развертыванию производства щитового оборудования. Это будет мультибрендовое изделие, но продукт будет российским. Следующий этап – локализация производства генераторных установок. Компания взаимодействует с молодым амбициозным европейским производителем, имеющим ноу-хау по сборке генераторных установок.

Мы работали, работаем и планируем работать, не прекращая своего развития, соответствуя требованиям меняющегося рынка, в том числе запросам на локализацию производства в России.

Edge как эволюция ИТ

После десятилетия централизации ИТ маятник качнулся в другую сторону, и все больше компаний формируют сети узлов распределенных вычислений, приближенных к конечным устройствам. О тенденциях и решениях в области Edge Computing – Денис Шарапов, менеджер по развитию направления «Модульные центры обработки данных» подразделения IT Division компании Schneider Electric.

Денис Шарапов

– Каковы причины интереса заказчиков к решениям Edge Computing?

– В основе этого процесса – общее развитие ИТ и повышение требований к отказоустойчивости информационных систем. Растут объемы генерируемой и передаваемой информации, увеличивается спрос на широкополосные каналы связи, а телеком-инфраструктура далеко не всегда и не везде способна удовлетворить этот спрос. Даже фанаты облачной модели поняли, что все в облако выносить нецелесообразно, а порой просто невозможно. Несмотря на многочисленные преимущества облаков, некоторые процессы логично оставлять на собственной площадке – по причине чувствительности к задержкам, из соображений безопасности и доступности данных, положений государственного регулирования и т.д.

Все чаще компании приходят к выводу о необходимости дополнения централизованной (облачной) модели системой граничных вычислений, что позволяет оптимальным образом выстроить ИТ-систему. Формируется гибридная модель, согласно которой часть процессов выполняется в узлах Edge Computing – максимально близко к конечным элементам. В них осуществляется, так скажем, тактическая обработка сырых данных, а уже ее результаты отправляются в центральный ЦОД для стратегической обработки.

– Каков портфель предложений Schneider Electric для Edge Computing?

– Сегодня компания поставляет все основные элементы инженерной инфраструктуры, от стоек и шкафов до сложнейших систем бесперебойного электропитания, охлаждения и ПО управления. Все это может быть интегрировано на месте в комплекс инженерной инфраструктуры. Но возможна и поставка в виде законченного и протестированного на заводе решения, так называемого prefab-ЦОДа. Типичные примеры «префабов» – микроЦОДы, которые и служат основой построения узлов граничных вычислений.

Развитие технологий позволило существенно увеличить вычислительную мощность одной стандартной стойки. Задачи, которые раньше требовали десятка стоек, сегодня могут быть успешно решены комплексом из одной-двух стоек. При этом надежность такого комплекса выше, чем серверной, построенной по старинке. Его можно сконфигурировать в соответствии с требованиями Tier II или Tier III. Если ранее подобный уровень отказоустойчивости достигался только в больших (централизованных) ЦОДах, то теперь он может и должен быть обеспечен и в микроЦОДах, формирующих узлы Edge Computing.

В зависимости от ситуации заказчикам требуются разные по масштабу микроЦОДы. Если для размещения ИТ-оборудования достаточно одного стойко-места, то оптимальным вариантом из портфеля Schneider Electric будет линейка микроЦОДов SmartBunker. Модельный ряд SmartBunker делится на три группы продуктов. Модели SX предназначены для ИТ-помещений, а потому в них нет собственной активной системы охлаждения. Решения CX оптимизированы для установки в офисах, они имеют дополнительную звукоизоляцию и укомплектованы вентиляторами. Наконец, для производственных площадок предлагаются микроЦОДы SmartBunker FX в корпусе с дополнительной физической защитой, оснащаемые различными вариантами активных систем охлаждения. Многослойный стальной каркас с уплотнителями и изоляционными панелями позволяет защитить установленное внутри оборудование от несанкционированного доступа, негативных факторов окружающей среды, вибрации и пр.

Если на уровне Edge Computing необходимо установить больше вычислительных средств, то мы можем предложить заказчику ЦОДы в корпусном исполнении контейнерного типа. Это продукты SmartShelter Container, которые построены на основе стандартных (6–12-метровых) контейнеров и вмещают до 14 стоек с ИТ-оборудованием. Важные преимущества решений на базе стандартных контейнеров – удобство транспортировки и невысокая стоимость. С целью упрощения обслуживания шкафы устанавливаются на специальные салазки для возможности их перемещения и обеспечения полноценного доступа к ИТ-оборудованию. Такие контейнеры обладают высоким уровнем защиты и могут размещаться и эксплуатироваться в неблагоприятных внешних условиях.

– Каковы особенности инженерной «начинки» решений для Edge Computing?

– В Edge-ЦОДах используются инженерные решения, которые по уровню технологичности, надежности и эффективности не уступают решениям, применяемым в больших (облачных) ЦОДах. При этом в предлагаемые Schneider Electric микроЦОДы могут быть установлены как традиционные, так и ультрасовременные инженерные системы.

В небольших ЦОДах желательно использовать максимально компактные инженерные компоненты, что позволит оптимизировать размещение полезной нагрузки и увеличить место, выделяемое под ИТ-оборудование. Если гово-

рить о системе бесперебойного электропитания, то наиболее наглядный пример – ИБП с компактными и относительно нетяжелыми литий-ионными батареями. Начав несколько лет назад выпуск некоторых моделей своих трехфазных ИБП большой мощности с литий-ионными аккумуляторами, в конце 2017 г. мы анонсировали ИБП малой мощности с таким же типом накопителей энергии.

Для систем охлаждения есть множество вариантов, в том числе с фрикулингом. Когда заказчику необходимо разместить одну стойку мощностью, скажем, до 3 кВт, скорее всего ему нет смысла прибегать к дорогостоящим «зеленым» технологиям охлаждения. В этом случае бывает достаточно приточно-вытяжной вентиляции, уже имеющейся в здании. Если требования к энергооснащенности стойки высокие, то можно применить архитектуру охлаждения закрытого цикла.

В микроЦОДах на десятки киловатт экономия от использования «зеленых» технологий уже будет существенной, и стоит проанализировать целесообразность установки более энергоэффективных решений. Вариантов фрикулинга также множество. Например, для инсталляций в местах с относительно чистым воздухом можно задействовать недорогие моноблочные кондиционеры с функцией прямого фрикулинга (подмеса наружного воздуха). Такие кондиционеры размещаются снаружи контейнера и не занимают полезное место внутри. Для менее благоприятной, урбанистической и индустриальной среды мы можем предложить несколько вариантов систем непрямого фрикулинга или механическое охлаждение на «теплой воде».

– Существует мнение, что для Edge Computing оптимальны уже упомянутые вами prefab-ЦОДы.

– Edge – не обязательно «префаб». Это может быть и классическое решение, с поэлементной сборкой и тестированием на объекте. Однако все чаще заказчики делают выбор в пользу prefab-ЦОДов благодаря таким их преимуществам, как сокращение сроков реализации проектов, предсказуемые гарантированные характеристики и пр.

В случае удаленных инсталляций важно еще и то, что при использовании подготовленных на заводе решений не нужно тратить время и средства на командировку специалистов высокого уровня на место установки. Более того, в prefab-ЦОД может быть установлено предварительно сконфигурированное ИТ-оборудование, а на месте достаточно распаковать его и подключить к сети передачи данных.

Вот лишь один пример: за основу младшей модели микроЦОДов SmartBunker SX взята стойка NetShelter SX версии SP, сертифицированная компанией Cisco на безопасную установку и транспортировку с уже интегрированными компонентами конвергентной инфраструктуры Cisco UCS. Использование таких решений, несомненно, упростит и удешевит развертывание Edge-узлов в проектах с территориально распределенной сетью филиалов или офисов.

– Сталкивались ли вы с запросами на мобильные решения Edge Computing? Каковы технические особенности таких решений?

– Мобильными решениями интересуются многие, но реальных заказчиков – единицы. Серьезная проблема подвижных ИТ-комплексов – наличие устойчивого канала связи и надежного электропитания.

Мобильные ЦОДы, конечно, существуют. Это сильно индивидуализированные проектные решения, которые реализуются под конкретного заказчика. В них, в частности, шкафы и корпуса устанавливаются на вибропоглощающие платформы, применяется и множество других специальных средств защиты. Но надо понимать, что комплекс мер, необходимых для эксплуатации ИТ-оборудования на подвижных составах, водном транспорте и т.д., недешев и он не ограничивается защитой ИТ-оборудования. Все инженерные системы подбираются и проектируются с учетом этой специфики среды размещения и эксплуатации.

– На какой стадии сейчас находится рынок Edge Computing? Есть ли примеры проектов?

– В прошлом году в СНГ было реализовано несколько десятков проектов для Edge Computing. Причем речь идет не об инсталляции отдельных инженерных элементов, например ИБП, а о реализации комплексных Edge-решений, в том числе на базе prefab-ЦОДов. Глобальный опыт Schneider Electric на порядок больше. Среди публичных кейсов наиболее крупные проекты – это сети, например, McDonalds и Gap. Речь идет о развертывании микроЦОДов производства Schneider Electric в первом случае – непосредственно в ресторанах сети точек быстрого питания, а во втором – в магазинах торговой сети.

– По-видимому, в перспективе часто будут использоваться гибридные схемы с центральным ЦОДом и множеством распределенных Edge-ЦОДов. Как Schneider Electric может помочь в реализации и эксплуатации таких гибридных схем?

– Предложения Schneider Electric не ограничиваются физической инфраструктурой. Комплексный подход и широкий ассортимент позволяют развернуть программно-аппаратную инженерную экосистему EcoStruxure с соответствующим требованиям заказчика отраслевым «уклоном». Она состоит из трех уровней. На нижнем – оконечные устройства (различные исполнители, приводы, датчики, автоматика, рабочие места и т.д.), которые обладают определенным уровнем интеллекта – они обеспечивают производственный процесс и его базовую автоматизацию. Выше – тот самый уровень Edge, на котором располагаются ИТ-комплексы, контролирующие оконечные устройства и обеспечивающие обработку «сырых» данных. Еще выше – уровень стратегического анализа данных, который, как правило, реализуется в больших ЦОДах. Замечу, что сбор и анализ данных с большого числа ИТ-площадок позволяет оптимизировать обслуживание инженерных комплексов и принять превентивные меры для предотвращения аварий и недопущения ухудшения характеристик, что в итоге повысит надежность и эффективность ИТ и производства в целом.

OpenStack: жизнь после хайпа

Николай Носов

OpenStack преодолел пик завышенных ожиданий кривой зрелости технологий Gartner и прошел точку разочарования.

В конце 2016 г. две ведущие компании проекта провели сокращения. Hewlett Packard Enterprise уволила команду разработки OpenStack, а компания Mirantis число своих сотрудников сократила на треть. Весной 2017 г. компания Intel отказалась от сотрудничества с Rackspace и прекратила финансирование совместного инновационного центра по разработке приложений OpenStack.

Впрочем, компании Rackspace и Mirantis работы в рамках экосистемы OpenStack продолжили, а Intel в конце 2017 г. даже анонсировала новый проект – Kata Containers. Не прекращали работу и другие игроки, так что технология продолжала развиваться и сейчас выходит на плато производительности (рис. 1). Шума вокруг облачной платформы с открытым исходным кодом стало меньше, но внедрения продолжаются. OpenStack по-прежнему активно используется в крупном бизнесе.

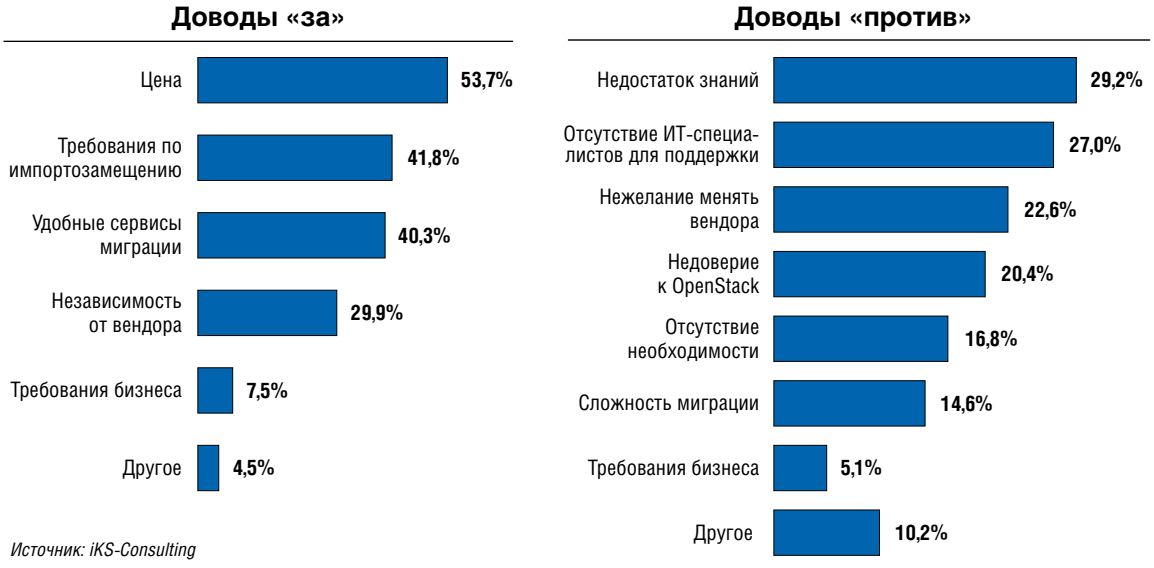
Рис. 1. Кривая зрелости технологий Gartner

Были и позитивные новости. Летом 2017 г. о переходе на OpenStack заявил крупнейший в мире регистратор доменных имен Go Daddy. В настоящее время сообщество OpenStack Foundation насчитывает 84 тыс. участников из 179 стран. Проект поддерживают 670 компаний, в числе которых такие гиганты индустрии, как AT&T, Huawei, SUSE, ZTE, Rackspace, Intel, Cisco, NetApp, Red Hat, Ericsson. На платформе OpenStack реализован ряд проектов NASA, Yahoo, Гарвардского университета и Массачусетского технологического института, а также часть проектов по разработке адронного коллайдера CERN. Корпоративными пользователями OpenStack являются компании Wells Fargo, Visa, American Express, Walmart, Target, Gap, eBay, PayPal, BMW, Volkswagen и GE. Крупнейшие глобальные компании, не желающие зависеть от поставщиков проприетарных облаков, по-прежнему оказывают поддержку проекту.

OpenStack в России

Новости из России приходили неоднозначные. Закрыла свои подразделения в нашей стране компания Mirantis. В 2017 г. не состоялась ежегодная конференция OpenStack Day, хотя еще в 2015-м и 2016-м дни рождения OpenStack отмечались у нас с размахом.

Но были и достижения. В 2017 г. компания RU-Center запустила платформу предоставления услуг аренды виртуальных серверов (VDS/VPS) на основе облачной инфраструктуры



Источник: iKS-Consulting

Рис. 2. Что способствует и что препятствует переходу на OpenStack

OpenStack, а осенью о запуске своего B2B-сервиса виртуальной облачной инфраструктуры Infra Mail.Ru на базе OpenStack заявила компания Mail.Ru. Облачную платформу использует для тестовых сред Сбербанк, развернул свое облако на OpenStack «Ростелеком». Наша страна стала играть заметную роль в мировом сообществе, а координатор российского сообщества OpenStack Илья Алексеев стал OpenStack Ambassador (региональным координатором по России и странам СНГ).

Предпосылки для использования платформы в России есть. Привлекательно выглядит OpenStack для решения задач импортозамещения. Например, в Китае на базе открытого кода OpenStack построила свое облако компания Huawei – и стала лидером на рынке частных облаков страны. Если внимательно посмотрим на архитектуру решения Huawei FusionCloud для построения распределенного облачного ЦОДа (закрывает четыре слоя: инфраструктура, слой пулов ресурсов, слой управления и слой каталогов услуг), то увидим знакомые блоки из OpenStack – контроллер, управляющий работой виртуальных машин Nova, компонент для подключения к сети Neutron, блочное хранилище для гостевых виртуальных машин Cinder, службу bare metal Ironic и распределенную систему хранения Swift.

Как показывает проведенный в 2017 г. опрос iKS-Consulting, в России наиболее важным фактором при выборе платформы OpenStack является цена (53,7%) и лишь потом идут требования по импортозамещению (41,8%) (рис. 2). Для крупного бизнеса затраты на лицензии при покупке проприетарных решений существенно больше, чем расходы на поддержку облачной платформы с открытым кодом, и фактор цены становится решающим.

> В России наиболее важным фактором при выборе платформы OpenStack является цена и лишь потом идут требования по импортозамещению

В принципе интерес к облачной платформе должен проявлять госсектор, для которого важно наличие исходного кода. Но госсектор не может позволить себе иметь штат сопровождающих систему программистов. Активно занимается разработками в проекте российская компания Hystax, создает свою облачную платформу для госорганов на базе OpenStack компания «Тионикс», но в целом выбор российских коммерческих компаний сильно ограничен. В итоге задумывающиеся об импортозамещении компании зачастую выбирают китайских вендоров.

Другими доводами в пользу использования облачной платформы являются удобные сервисы миграции (40,3%), а также независимость от вендора (29,9%). Главные барьеры на пути перехода к OpenStack – недостаток знаний о платформе (29,2%), отсутствие ИТ-специалистов по поддержке (27%) и нежелание менять уже хорошо работающую систему. Отдельно стоит выделить недоверие к платформе (20,4%), которое отчасти объясняется негативным опытом эксплу-

МНЕНИЕ ЭКСПЕРТА

OpenStack и проблема ответственности

Проводя опрос конечных пользователей по системам виртуализации, мы часто слышали про проблему ответственности. Используя открытое решение, ИТ-руководитель часто остается один на один с проблемами, которые могут возникать в ходе его эксплуатации. Конечно, существует огромное сообщество пользователей, которые могут помочь советом, но решение конкретных вопросов ложится на плечи данного ИТ-подразделения. При использовании брендированных продуктов часть ответственности перекладывается на службу поддержки соответствующего производителя, и ИТ-руководитель предприятия чувствует себя увереннее. Это основная причина, препятствующая более широкому внедрению OpenStack, несмотря на все его преимущества: низкую стоимость, открытость кода, независимость от конкретного поставщика и т.д.

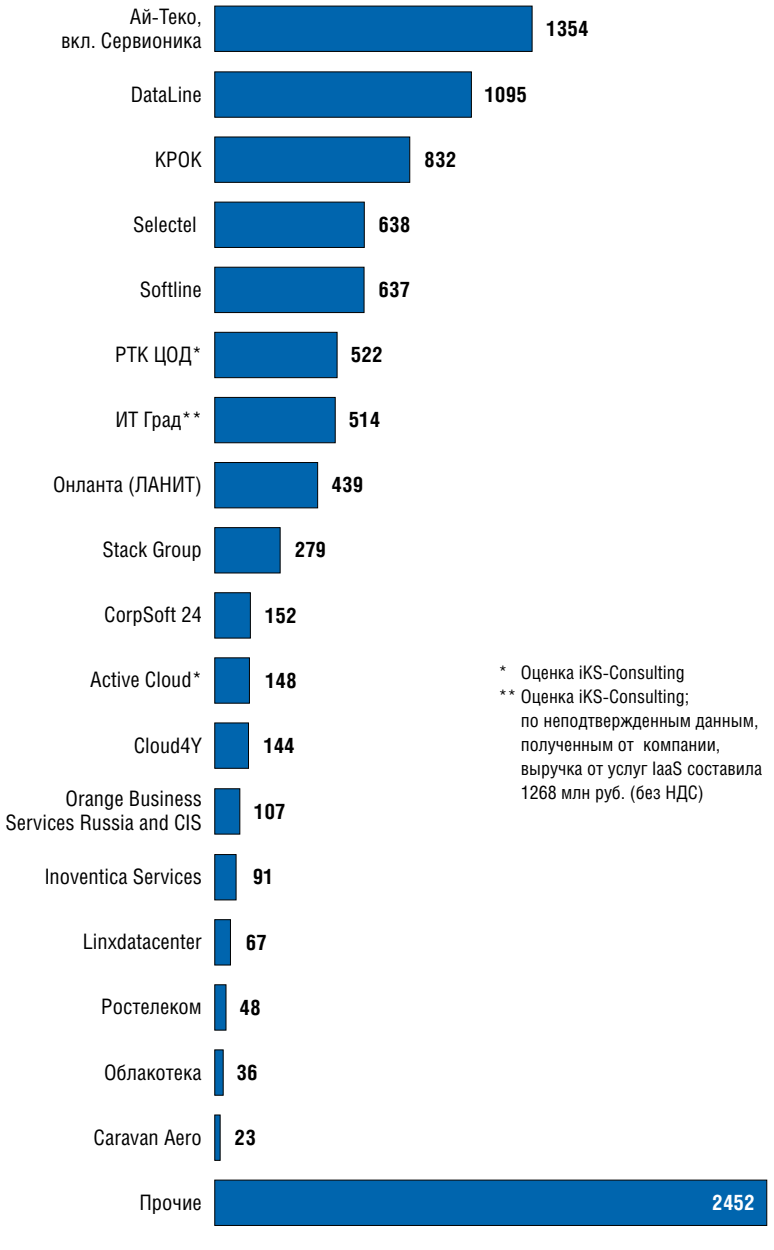
На мой взгляд, решения на базе OpenStack будут востребованы у облачных провайдеров. Во-первых, они располагают штатом квалифицированных специалистов, которые могут развивать и поддерживать этот продукт. Во-вторых, предложения провайдера на базе бесплатного ПО будут дешевле, а следовательно, более конкурентоспособны на рынке и привлекут большее число пользователей, которые не озадачены соблюдением жестких требований и предписаний по использованию конкретного ПО. Кроме того, открытость OpenStack и независимость от западных производителей делают его более привлекательным для госзаказчиков, которые должны следовать требованиям программ импортозамещения и иметь надежную защиту от возможных западных санкций.

Станислав Мирин, ведущий консультант, iKS-Consulting

атации других свободно распространяемых программных продуктов.

Крупнейшие российские игроки рынка IaaS в области публичных и гибридных облаков тоже используют OpenStack (рис. 3). Так, входящая в ГК «Ай-Теко» компания «Сервионика» еще в 2012 г. запустила публичное облако MakeCloud на базе OpenStack. Озаботившись снижением стоимости содержания облака для заказчиков, в 2013 г. «Сервионика» создала гибридное решение: комбинированное облако из eCloud (VMware) и MakeCloud. А входящая в пятерку лидеров компания Selectel с 2014 г. предлагает на базе OpenStack услугу «Виртуальное приватное облако».

Рис. 3. Крупнейшие игроки IaaS по выручке от услуг в публичных и гибридных облаках (млн руб.), 2016 г.



Источник: iKS-Consulting

OpenStack и Edge Computing

По своей сути OpenStack – это механизм интеграции с открытым исходным кодом, который предоставляет API-интерфейсы для управления bare metal, ресурсами виртуальной машины и контейнера в одной сети. Стоит отметить популярность OpenStack в ЦОДах телекоммуникационных провайдеров. В 74 дата-центрах по всему миру платформу использует крупнейшая телекоммуникационная компания AT&T. Активно эксплуатируют платформу Orange и Swisscom, китайские телеком-операторы (China Mobile, China Telecom, China Unicom) и немецкая Deutsche Telekom.

> Главные барьеры на пути перехода к OpenStack – недостаток знаний о платформе, отсутствие ИТ-специалистов по поддержке и нежелание менять уже хорошо работающую систему

Традиционно облако было ориентировано на центр обработки данных, но с развитием Edge Computing и SDX появились потребности расширить возможности управления инфраструктурой до края сети. Летом 2017 г. на саммите OpenStack в Бостоне компания Verizon предложила cloud-in-a-box – программно-аппаратное решение на базе OpenStack для Edge Computing. Клиент получает маленькое облако на границе сети с программно определяемой виртуализированной ИТ-инфраструктурой, управляемое из основного ЦОДа. Оркестрация происходит не только в основном дата-центре, но и по всей сети. Главное преимущество такого решения – гибкость. Клиенту не нужно покупать новое оборудование для Edge-ЦОДа при необходимости изменения его конфигурации.

Управлять большим количеством облаков с разными API – сложная задача. «Для Edge Computing, где используется много маленьких облаков, важна стандартизация. Ее может обеспечить имеющая большое количество открытых API платформа OpenStack, которая уже стала стандартом де-факто при реализации частных облаков», – считает И. Алексеев. Он сообщил, что в OpenStack Foundation уже создана рабочая группа по использованию облачной платформы для Edge Computing.

Технология прошла период хайпа и точку разочарования. Теперь можно трезво оценить ее возможности, достоинства и недостатки. Облачная платформа не победила проприетарных конкурентов, но нашла свои рыночные ниши, где будет развиваться. ИКС

Рынок ИБП: заметный рост во всех сегментах

Андрей Маркин

Развитие автоматизации различных сфер экономики, бизнеса и жизни людей привело к существенному расширению круга отраслей, активно использующих источники бесперебойного питания. Об этой и других тенденциях на рынке ИБП – Андрей Маркин, глава представительства Powercom в России, Беларуси и Казахстане.

– Тенденций, наметившихся в прошлом году и актуальных для нынешнего, хочется назвать как минимум три. Во-первых, российский рынок ИБП ожил и продемонстрировал существенный рост во всех сегментах. Так, канальные продажи Powercom увеличились почти на 40% (здесь и далее указан рост продаж в долларах. – *Прим. ред.*). Цифра эта выше среднерыночных показателей и говорит о грамотно выстроенной работе с партнерами.

Весьма заметным трендом стало оживление спроса на ИБП в регионах. По итогам 2017 г. на долю региональных продаж Powercom пришлось 52%, тогда как в 2016-м этот показатель не дотягивал и до 50%. Заметно выросли продажи сразу в нескольких округах, например в Уральском, Дальневосточном, Приволжском, Центральном и Северо-Западном (перечислены в порядке убывания величины прироста в натуральном выражении), – они не просто увеличили свою долю, а вышли на абсолютный максимум за последние три года.

И наконец, третий тренд – изменение в структуре продаж ИБП. Неуклонно увеличивается объем продаж источников бесперебойного питания мощностью выше 1 кВА (рост более 30%), в частности онлайновых (13,5%), причем как в денежном, так и в штучном выражении. Мы считаем, что эта тенденция в немалой степени обусловлена расширением сфер применения ИБП вследствие развития автоматизации и роботизации различных сфер экономики, бизнеса и жизни человека.

– Как рыночные тенденции отразились в новых разработках Powercom?

– Продуктовая линейка Powercom традиционно велика, и мы можем предложить оборудование для решения самого широкого круга задач – от частного применения и защиты газовых котлов до обеспечения бесперебойного питания серьезного промышленного оборудования и коммерческих ЦОДов. Наблюдая рост интереса к сегменту онлайновых ИБП и расширение отраслевого применения ИБП, мы, конечно же, наращиваем свою экспертизу и конкурентоспособность в этом сегменте.

В прошлом году с появлением ИБП Vanguard второго поколения (VGD-II-33) полностью обновилась линейка трехфазного оборудования. Модели оказались удачными, быстро привлекли к себе внимание и завоевали доверие заказчиков. В этом году готовим полное обновление однофазных онлайновых ИБП (мощностью до 3 кВА), относящихся к категории часто запрашиваемых и весьма востребованных на рынке.

– Каковы основные конкурентные преимущества ИБП Powercom?

– Тридцатилетний опыт производства и плотное общение с партнерами и заказчиками позволяют нам быть в курсе не только трендов рынка, но и реальных потребностей бизнеса. Это, в свою очередь, дает возможность вовремя обновлять оборудование, подстраивая свою линейку под требования сегодняшнего дня. Причем у наших партнеров и клиентов всегда есть возможность обратиться к нам за кастомизированным заказом. Для некоторых партнеров мы выпускаем специальные серии ИБП, которые лучше соответствуют тем или иным потребностям. Такие ИБП могут отличаться количеством или типом розеток, иметь плавкий предохранитель, оснащаться дополнительными коммуникационными разъемами и т.п. Наши продукты демократичны по цене, хорошо зарекомендовали себя на рынке, а сеть сервисных центров охватывает все уголки нашей страны.

– Использует ли Powercom в своих ИБП литий-ионные аккумуляторные батареи? В чем их преимущество?

– Массово мы пока не запустили производство ИБП с литий-ионными аккумуляторными батареями, но выпускать такие устройства под заказ уже готовы. Основные преимущества хорошо известны: увеличенный срок службы, быстрая зарядка аккумуляторов, уменьшение размеров и веса. Единственное препятствие для перехода на производство ИБП с литий-ионными аккумуляторами – цена. Сами АКБ пока остаются дорогим удовольствием, и это серьезно сказывается на стоимости всего ИБП. Финансовую выгоду можно увидеть только в совокупной стоимости владения за несколько лет вперед, однако далеко не каждый заказчик готов к таким расчетам. Да и кризисный период не способствовал переходу на более дорогое оборудование.

– Каковы планы Powercom по дальнейшему развитию продуктов? Есть ли в этих планах место альтернативным источникам электроэнергии?

– Наша компания производит солнечные панели, инверторы, системы мониторинга и учета выработки электроэнергии и т.д., а также имеет экспертные знания и множество реализованных проектов строительства и обслуживания солнечных электростанций в Европе, США, странах Азии и Африки. Надо сказать, что Powercom отлично зарекомендовал себя на рынке альтернативных источников электроэнергии. Но, к сожалению, в России это направление активного развития не получило. Только сейчас разрабатывается нормативная база по поддержке возобновляемых источников энергии, предназначенных для частных потребителей. Словом, за развитием событий следим и будем готовы выйти на этот рынок в любой момент.

Индустриализация – сегодня, открытые архитектуры – завтра

Об основных тенденциях в области ЦОДостроения мы поговорили с Ольгой Антиповой, генеральным директором «АДМ Партнершип» – ведущей российской компании, работающей в области проектирования, управления и реализации сложных инженерных объектов.

Ольга Антипова

– Одна из ключевых тенденций, которые оказывают существенное влияние на проектирование и строительство ЦОДов, – индустриализация решений для дата-центров. Все чаще в проектах используются заранее подготовленные и протестированные на заводах модули и блоки высокой заводской готовности – на профессиональном жаргоне их называют префабами (от англ. prefabricated). Применение таких решений позволяет существенно сократить время реализации проектов, а также гарантирует заранее просчитанные характеристики ЦОДов.

Вторая тенденция – растущий интерес заказчиков к так называемым моновендорным ЦОДам. Принцип получения основных систем и экспертизы «из одних рук» дает ряд важных преимуществ и становится все более востребованным, особенно при строительстве корпоративных дата-центров.

Заказчики начинают интересоваться и решениями, построенными в соответствии с открытыми архитектурами, в первую очередь теми, что предлагаются в рамках проектов OCP (Open Compute Project) и Open19. В перспективе такие решения позволят не только снизить себестоимость ИТ-объектов, но и повысить их энергоэффективность.

– Давайте подробнее обсудим названные тенденции и начнем с модульных ЦОДов на основе «префабов». Ранее считалось, что это гораздо более дорогие решения по сравнению с традиционными. Ситуация изменилась?

– Вы правы в том, что еще несколько лет назад модульные ЦОДы были существенно, порой в несколько раз дороже ЦОДов, реализуемых традиционно, т.е. с капитальным строительством (или реконструкцией) здания, проектированием с нуля, поэлементным монтажом, тестированием на площадке и пр. Однако с ростом популярности модульных решений растут и объемы их производства, а значит, снижается стоимость.

Кроме того, важно оценивать не только стоимость отдельных продуктов, но и общую стоимость развертывания центра обработки данных. Модульные ЦОДы часто разворачивают в «чистом поле» или в быстровозводимом легком здании, например в ангаре. В этом случае значительно сокращается количество разного рода согласований и формальностей, на которые уходит масса времени и ресурсов при капитальном строительстве или реконструкции здания под ЦОД.

Использование типовых модулей существенно сокращает расходы на проектирование. Для нас как для проектировщиков чрезвычайно значимы такие преимущества, как вариативность проектных решений и возможность гибкого планирования развития объекта.

В условиях, когда заказчики очень трепетно относятся к выделению финансирования, все более важной становится возможность наращивания мощности ЦОДа по мере необходимости. В нынешней ситуации мало кто готов сразу строить весь ЦОД на дальнюю перспективу. Компании предпочитают тратить средства поэтапно. А для такого подхода модульные решения – оптимальный выбор.

В итоге, по моей оценке, при учете всех составляющих проекта, включая проектирование, инсталляцию и т.д., расходы на модульные и традиционные ЦОДы сегодня сопоставимы.

– Значит ли это, что с учетом других преимуществ модульных решений классический подход сдает позиции?

– Я бы не стала сталкивать лбами два подхода, свои преимущества и недостатки есть у каждого из них. Они не конкурируют, а скорее дополняют друг друга. Так, в классических ЦОДах все больше систем строится по модульному принципу. На рынке представлено немало prefab-модулей с инженерными системами, например модули электропитания или охлаждения, в том числе экономайзеры.

Подобные модули можно оперативно стыковать к уже существующим ЦОДам, обеспечивая дополнительные ресурсы электропитания или охлаждения. Это бывает очень актуально, поскольку нередки ситуации, когда площади для размещения ИТ-оборудования в ЦОДе еще есть, а, скажем, мощности системы бесперебойного питания исчерпаны. Возможна и обратная ситуация: ресурсы инженерной инфраструктуры еще в избытке, а площади закончились. В таких случаях ничто не мешает устанавливать внешние ИТ-залы, выполненные в стандартных или специализированных контейнерах. В любом случае получается экономически выгодное гибридное решение.

Спрос на «префабы» будет расти, в том числе благодаря развитию периферийных вычислений – Edge Computing. Для таких проектов требуется максимально приблизить

вычислительные мощности к конечным устройствам, например к производственной площадке. Для этого наилучшим решением часто являются микроЦОДы, выполненные в формфакторе одной стойки или в виде модуля, содержащего несколько стоек. Такие комплексные решения оснащаются всеми необходимыми инженерными элементами, включая средства бесперебойного электропитания и охлаждения.

– Вместе с темой микроЦОДов, которые часто построены на основе продуктов одного производителя, мы подошли ко второй обозначенной вами тенденции – моновендорным ЦОДам. В чем суть этого феномена?

– Четкого определения моновендорного ЦОДа нет. Как правило, под ним понимают объект, основные инженерные системы которого поставлены одним производителем. Это системы, обеспечивающие бесперебойное электропитание ИТ-оборудования, его охлаждение, а также размещение (шкафы и стойки), в том числе с выделением горячих/холодных коридоров и изоляцией воздушных потоков. К этим трем «китам» инженерной инфраструктуры ЦОДа часто добавляют единую систему управления, например класса DCIM (Data Center Infrastructure Management). Сегодня есть несколько крупных вендоров, способных поставить решения для таких моновендорных ЦОДов.

Но сразу следует сказать, что стопроцентно моновендорной инженерной инфраструктуры не бывает. Некоторые категории оборудования всегда поставляются специализированными производителями. Это, в частности, системы пожаротушения и дизель-генераторные установки. Причем важно обеспечить грамотную интеграцию таких решений в общую инфраструктуру ЦОДа.

Преимущества моновендорного подхода давно известны и по большому счету не привязаны к индустрии ЦОДостроения. Это отличная совместимость разных компонентов инфраструктуры, что снижает время на ее проектирование, реализацию и модернизацию. В случае работы с одним поставщиком может быть сокращено время поставки оборудования, лучше согласована последовательность его поступления на объект (чтобы можно было параллельно вести различные монтажные работы) и т.д. Важный плюс моновендорного подхода – возможность заключения единого сервисного контракта на обслуживание всей инфраструктуры. При этом не возникает ситуаций, когда один поставщик перекладывает ответственность на другого, ускоряется работа по выявлению и устранению неполадок, повышается надежность объекта в целом.

Конечно, у моновендорного подхода есть и недостатки. Ни один производитель не способен предложить лучшие варианты для всех абсолютно компонентов и подсистем. Всегда на рынке можно отыскать устройства с характеристиками получше, а собрав их воедино – получить систему с более высокими показателями. Но при этом потребуются существенные усилия и затраты на интеграцию, и не факт, что всё получится.

Полагаясь на моновендорный подход, заказчик оказывается привязанным к архитектуре, которую предпочитает выбранный вендор. Хотя, справедливости ради, стоит заметить, что у ведущих производителей имеются различные архитектурные варианты, например для систем охлаждения.

– А что с ценой? Какой вариант – моно- или мультивендорный – выгоднее заказчику?

– С одной стороны, будучи привязанным к одному вендору, заказчик может попасть в ситуацию, когда тот будет диктовать свои ценовые условия. С другой – закупка большого объема оборудования у одной компании – повод получить существенные скидки. Да и единый сервисный контракт может оказаться намного выгоднее нескольких, заключенных на обслуживание отдельных подсистем. Нельзя однозначно сказать, какой подход будет экономически более привлекательным – все зависит от специфики конкретного проекта и особенностей требований заказчика.

– Переходим к теме открытых архитектур. Она горячо дебатируется, но насколько такие решения востребованы на практике?

– В основном обсуждаются два подхода: OCP и Open19. Инициатором первого выступила компания Facebook, которая уже давно сама занимается разработкой оборудования для своих ЦОДов. На каком-то этапе она решила сделать свои разработки открытыми, и они стали активно развиваться мировым экспертным сообществом. Сегодня в проекте OCP участвуют порядка 50 корпоративных членов, в том числе ведущие производители инженерных систем для ЦОДов.

Среди основателей Open19 – компания LinkedIn, а в членах этого сообщества уже около 30 компаний. Ключевое отличие этой инициативы от OCP видно из ее названия: она предполагает использование более привычных для ИТ-сообщества конструктивов шириной 19”, тогда как предложения OCP базируются на формфакторе 21”.

Цели проектов схожи: сделать оборудование для ЦОДов (включая серверные платы, блоки питания, шасси, стойки, средства охлаждения) более удобным и доступным, упростить процесс его приобретения, установки и обслуживания, что в итоге позволит существенно снизить себестоимость дата-центров. Важно и то, что предлагаемые архитектуры оптимизируют размещение различных компонентов. А это даст возможность снизить энергопотребление отдельных систем и повысить энергоэффективность ЦОДа в целом.

Понятно, что озвученные цели привлекательны для владельца любого ЦОДа. Идеи OCP и Open19 сначала воплощаются в жизнь на объектах интернет-гигантов уровня Facebook и LinkedIn, но постепенно они дойдут и до менее масштабных ЦОДов. Российские заказчики интересуются такими решениями, кто-то даже тестирует их, но о каких-либо масштабных внедрениях мне пока неизвестно. Но перспективы вполне реальны.

Макропоказатели ЦОДа: проектируем на коленке

Андрей Павлов, генеральный директор, «ДатаДом»

Многие сталкивались с ситуацией, когда нужно оперативно рассмотреть возможность строительства ЦОДа на той или иной площадке. Как приблизительно оценить технические характеристики будущего объекта и его стоимость?

Работая более 15 лет в отрасли ЦОДов и не владея глубоко приемами проектирования инженерных систем, я вывел для себя ряд эмпирических закономерностей, позволяющих существенно упростить решение данной задачи на уровне руководителя.

Как правило, при осмотре объекта у заказчика возникают такие вопросы: «сколько здесь можно разместить оборудования?», «каковы необходимые площадь и энергомощность?», «сколько это может стоить?». Очевидно, что без разработки детального технического задания, без полного понимания разнообразия вариантов технических решений для реализации инженерных систем ЦОДа и без формирования проектной документации точные ответы на поставленные вопросы получить затруднительно. Но порядок цифр, который, собственно, и интересует заказчика, оценить вполне можно. Часто достаточно таких ответов, как «20–25 стоек», «300–350 кВт» или «17–19 млн руб.».

Последовательность действий при подобной оценке следующая:

- определение мощности, требуемой на одну стойку;
- определение количества стоек, которое можно разместить в выбранных помещениях;
- определение общей мощности, потребляемой ЦОДом, и номиналов оборудования отдельных инженерных подсистем;
- определение площадей, требуемых для внешних блоков инженерных систем;
- и наконец, определение бюджета строительства объекта.

Следует сразу оговорить некоторые детали подобной оценки, особенно ее финансовой составляющей. Стоимость разных моделей инженерного оборудования для дата-центров может существенно различаться в зависимости от бренда, страны производства, применяемых технологий и материалов. Различия могут быть также обусловлены комплектацией и дополнительными опциями. Поэтому точно определить стоимость строительства ЦОДа без разработки технического задания и хотя бы предварительной проработки проектных решений невозможно.

Например, стоимость системы мониторинга сильно зависит от требований к объему контролируемых параметров. Так, в ЦОДе, состоящем из 20 стоек, могут контролироваться такие параметры, как температура и влажность в коридорах, наличие напряжения на энерговводах. По протоколу SNMP могут собираться данные с оборудования ИБП, ДГУ и системы кондиционирования. Эта информация будет предоставляться пользователю через веб-интерфейс, а сообщения об авариях могут передаваться по GSM-каналу. Стоимость подобной системы может колебаться в пределах 300–800 тыс. руб. в зависимости от производителя и дополнительного функционала.

Но если заказчик захочет осуществлять мониторинг каждого блока розеток в каждой стойке, не говоря уже о контроле каждой розетки или управлении ими, то стоимость системы мониторинга может возрасти многократно, поскольку стоимость блока розеток на 20–25 портов с возможностью контроля только общего энергопотребления начинается от 40–60 тыс. руб. А таких блоков розеток нужно 40 штук, общей стоимостью порядка 2 млн руб.

Определение мощности потребления одной серверной стойки

По большому счету этот параметр должен задать заказчик, но нередко он сам не представляет четко, что собирается строить. В таком случае рекомендуется исходить из следующих предпосылок: если заказчик не планирует массово размещать в ЦОДе облачные структуры, виртуальные машины или оборудование для научных исследований, «крутящее» сложные вычисления, а предполагает устанавливать клиентское оборудование или собственные информационные системы, то мощность стойки принимается равной 5 кВт. Целесообразность такого выбора подтверждена многочисленными статистическими данными, полученными от коммерческих дата-центров.

При необходимости увеличить мощность, потребляемую одной стойкой, количество стоек, которые можно разместить в конкретном помещении, и иные характеристики ЦОДа можно будет пересчитать с помощью несложного алгоритма.

Определение количества стоек для размещения в выбранных помещениях

Я неоднократно сталкивался с желанием заказчика создать ЦОД в самых необычных помещениях, например на этажах недостроенной те-

лебашни круглого сечения, в эркерах, подвалах неправильной формы и т.д. Оценивать такие помещения с точки зрения количества устанавливаемых в них серверных стоек существенно сложнее, чем обычные прямоугольные, – здесь нужна немалая инженерная фантазия. Поэтому остановимся на традиционных площадках. Следует только иметь в виду, что вместимость любых помещений неправильной формы будет на 20–50% меньше, нежели обычных.

Рассмотрим планировку типового ЦОДа на 96 стоек размером 600×1000 мм (рис. 1). Помещения для ИБП и АКБ на данном этапе не учитываем.

Для простоты расчетов предположим, что ряды стоек будут располагаться параллельно короткой стороне помещения. Для больших помещений такой подход с высокой долей вероятности приводит к более удобной компоновке оборудования в машинном зале. Кроме того, он облегчает соблюдение ограничения на максимальное расстояние от серверного оборудования до внутренних блоков системы кондиционирования. Для небольших помещений данное ограничение несущественно, и погрешность в оценке количества стоек становится небольшой.

Следующий этап – расположение холодных и горячих коридоров. Расстановка стоек по коридорам ограничивается традиционными размерами выпускаемых плит фальшпола, габаритами стоек и эргономическими требованиями к ширине проходов между рядами. Как правило, размеры плит фальшпола составляют 600×600 мм, габариты (Ш×Г) серверных стоек – 600–800 ×800–1200 мм. Для стоек мощностью до 5–7 кВт ширину холодного коридора принимают равной ширине двух рядов вентиляционных плит, а ширину горячего коридора – 1000 мм для стоек глубиной также 1000 мм (рис. 2).

Безусловно, при выборе ширины коридоров между рядами стоек возможна масса вариаций. Можно уменьшить горячий коридор до 800 мм и даже до 600 мм, используя двойные распашные двери и забывая об удобстве обслуживания. Можно устанавливать стойки не по линии стыка двух рядов плит фальшпола. Но все эти варианты стоит рассматривать лишь в ходе детального проектирования, при нехватке пространства для размещения оборудования.

Расположение рядов стоек описывается следующим образом:

- не менее 3,2 м для одного ряда стоек;
- не менее 5,2 м для полноценного холодного коридора (т.е. холодный коридор, два ряда стоек и два горячих коридора);
- каждый следующий холодный коридор (два ряда стоек, холодный коридор и горячий коридор) – плюс 4,2 м;
- каждый следующий ряд стоек (и холодный коридор) – плюс 2,2 м.

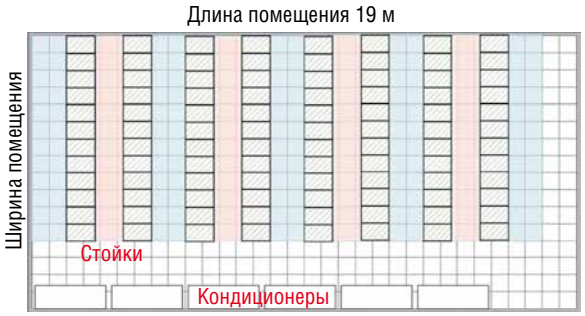


Рис. 1. Общий вид машинного зала на 96 стоек

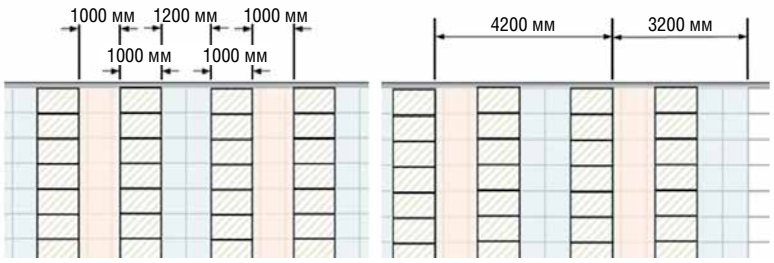


Рис. 2. Типовые размеры коридоров в серверном зале ЦОДа

На основании этих данных при первичной оценке вместимости помещения можно рассчитать количество N холодных коридоров (два ряда стоек на коридор), которые можно разместить в помещении заданной длины L, используя формулу:

N = (L – 5,2) / 4,2 + 1.

Например, в помещении длиной 19 м можно сформировать минимум (19 – 5,2) / 4,2 + 1 = 4 холодных коридора (восемь рядов стоек).

Теперь подсчитаем, сколько стоек можно разместить в каждом ряду. Мы приняли, что ширина стойки 600 мм, соответственно ширина каждого ряда будет составлять 0,6×К, где К – количество стоек в ряду. Кроме того, в торце каждого ряда могут быть установлены электрические распределительные щиты глубиной 300–400 мм. Далее нужно предусмотреть коридор для прохода персонала и проноса оборудования шириной не менее 1000–1200 мм и разместить внутренний блок системы кондиционирования глубиной 800–900 мм.

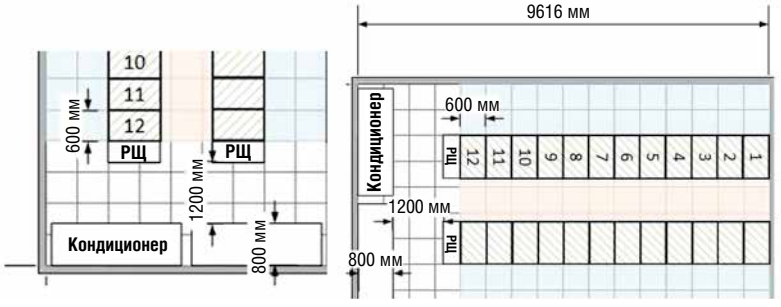
В итоге приблизительно 2–2,4 м по короткой стороне помещения занимают коридор для прохода, кондиционер и электрощит, а остальное пространство можно использовать под установку серверных стоек (рис. 3).

Количество стоек в ряду можно определить по следующей формуле:

K = (S – 2,4) / 0,6,

где S – ширина помещения.

Рис. 3. Типовые размеры для расчета числа стоек в ряду



Например, при ширине помещения S = 9,6 м количество стоек в ряду составит (9,6 – 2,4) / 0,6 = 12.

Однако необходимо помнить, что последнюю стойку в ряду рекомендуется располагать не далее 10–12 м от блока кондиционера. Это ограничение обусловлено физическими характеристиками распределения воздуха в подфальшпольном пространстве. Данные цифры не являются константой и зависят от высоты фальшпола, наличия препятствий воздушному потоку, напора кондиционера, но в большинстве типовых случаев их можно брать за основу. При расстоянии между последней стойкой и кондиционером более 10–12 м от следует запастись местом под установку второго ряда кондиционеров (+ 2 м к ширине зала).

В итоге получаем, что в нашем гипотетическом ЦОДе размерами 19×9,6 м можно разместить 12×4×2 = 96 стоек габаритами 600×1000 мм, и этот расчет совпадает с изначальным планировочным решением.

Есть более простой способ оценки вместимости ЦОДа. Он основан на статистических данных, полученных из реализованных проектов (табл. 1), и хотя он менее точен, чем произведенный нами расчет, но его погрешность вполне допустима для приблизительной оценки.

Построенные дата-центры (примеры 1–3) подтверждают статистические данные табл. 1. Однако не следует полагаться на приведенные цифры безоглядно, поскольку геометрия машинного зала – не единственный фактор, определяющий емкость ЦОДа. Нужное место в дата-центре занимает еще целый ряд объектов:

- пандусы и колонны;
- ИБП и системы АГПТ;
- помещения кроссовых;
- ГРЩ ЦОДа;
- хладоцентр.

В частности, по грубым прикидкам, площадь, необходимая для размещения ИБП и ГРЩ, составляет до 20% площади машинных залов.

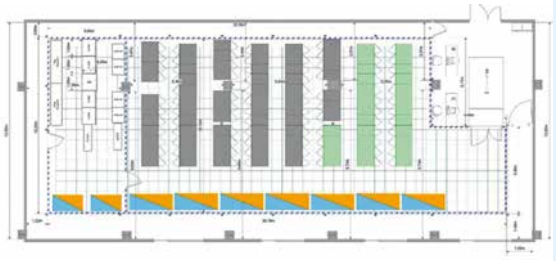
Таблица 1. Площадь, требуемая для размещения стоек в ЦОДе

Количество стоек, шт.	Площадь на одну стойку (для помещений правильной прямоугольной формы), кв. м/стойку
До 10	3–5
10–50	2,7–3
50–100	2,5–2,7
Более 100	2–2,5

Таблица 2. Средние размеры внутренних блоков фреоновых кондиционеров

Мощность, кВт	Габариты, мм
20–25	2000×1000×900
26–33	2000×1400×900
35–48	2000×1800×900
50–65	2000×2100×900
70–90	2000×2500×900

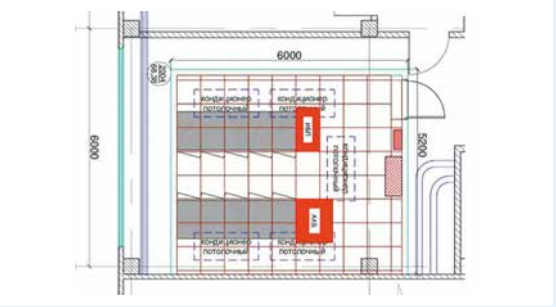
ПРИМЕР 1



Параметры площадки:

- 93 стойки по 5 кВт
- Площадь гермозоны – 250 кв. м
- Резервирование ИБП – до 2N
- Площадь на одну стойку – 2,7 кв. м

ПРИМЕР 2



Параметры площадки:

- 10 стоек по 5 кВт
- Площадь гермозоны – 31 кв. м
- Резервирование ИБП – N + 1
- Площадь на одну стойку – 3,1 кв. м

Кроме того, на плотность установки оборудования могут повлиять такие факторы, как увеличение времени автономии ИБП и мощности одной стойки: повышение мощности с 5 до 10 кВт повлечет за собой увеличение площади машинных залов и технических помещений внутри здания на 40–60%.

Оценка общей мощности ЦОДа

Для начала проведем верхнеуровневую оценку общей максимальной мощности потребления ЦОДа исходя из количества стоек, рассчитанного на предыдущем этапе, и средней мощности серверной стойки. Для упрощения расчетов сделаем несколько «директорских» допущений. В частности, примем, что потери на ИБП составляют 8–10%, потребление системы кондиционирования – 35% потребления стоек и ИБП (для фреоновых систем) и 45% – для чиллерных систем. Потребление остальных инженерных систем – 5% потребления стоек и ИБП.

Общее максимальное потребление ЦОДа ($P_{общ}$) рассчитывается по следующей формуле:

$P_{общ}$ = количество стоек × мощность стоек + потери на ИБП + потребление системы кондиционирования + потребление остальных систем.

Предположим, что у нас 30 стоек по 6 кВт. В этом случае:

потребление ИТ-оборудования = 30×6 = 180 кВт

потери на ИБП = 180×0,08 = 14,4 кВт

общее потребление ИБП + стойки = 180 + 14,4 = 194,4 кВт

потребление фреоновой системы кондиционирования = 194,4×0,35 = 68,04 кВт

потребление остальных систем 194,4 × 0,05 = 9,72 кВт

общее потребление ЦОДа = 194,4 + 68,04 + 9,72 = 272 кВт.

Оценка мощности системы кондиционирования и ее габаритов

Общая мощность охлаждения системы кондиционирования ($P_к$) рассчитывается по формуле:

$P_к$ = (потребление ИТ-оборудования + потери ИБП)×1,1,

где 1,1 – это запас.

При этом следует учитывать, что мощность одного шкафного фреонового кондиционера составляет в среднем 10–90 кВт. Кондиционеры мощностью до 40–50 кВт традиционно выпускаются в одноконтурном исполнении, что означает наличие одного компрессора и соответственно одного внешнего блока. Кондиционеры мощностью более 40–50 кВт – это уже двухконтурные машины (т.е. два компрессора и два внешних блока).

Средние размеры внутренних блоков фреоновых кондиционеров приведены в табл. 2 (у разных производителей эти параметры могут незначительно различаться).

Размер внешнего блока кондиционера мощностью 40–50 кВт составляет порядка 0,8–1×2,0–2,5 м. С учетом зоны обслуживания минимальная площадь, необходимая для установки внешнего блока мощностью 40–50 кВт, – 4 кв. м (2,5×1,5).

Исходя из опыта реализованных проектов (см. примеры 4 и 5), можно принять, что для размещения внешних блоков фреоновых кондиционеров требуется 30–35% площади машинных залов ЦОДа.

Расчет мощности ИБП и ДГУ

При расчете требуемой мощности источников бесперебойного питания (ИБП) и дизель-генераторной установки (ДГУ) будем использовать все те же «директорские» допущения.

Модель ИБП в общем случае подбирается исходя из мощности, потребляемой серверным оборудованием, с учетом параметра cos(f), который в среднем равен 0,85–0,95. Параметр cos(f) варьируется в зависимости от марки и модели оборудования. С мощностью ДГУ ситуация несколько более сложная. Для успешного запуска ДГУ в случае, когда одной из нагрузок является ИБП, следует учитывать коэффициент согласования (множитель), который колеблется в диапазоне 1,2–2. Такое требование обусловлено нелинейностью нагрузки ИБП, которая может оказывать существенное сопротивление запуску дизеля. Современные ИБП, построенные на IGBT-транзисторах, сократили необходимый запас мощности при выборе ДГУ, снизив коэффициент согласования до 1,2–1,5. Однако у разных производителей он может различаться. Чтобы уменьшить риск выбора ДГУ недостаточной мощности, в предварительных расчетах я рекомендую принимать коэффициент согласования равным 1,4.

ПРИМЕР 3

Параметры площадки:

- Восемь стоек по 5 кВт
- Площадь гермозоны – 24 кв. м
- Резервирование ИБП – до 2N
- Площадь на одну стойку – 3 кв. м

Расчет мощности ИБП проводится по формуле:

$P_{ИБП}$ (кВА) = количество стоек×мощность стойки (кВт) / cos(f).

Значение cos(f) выбирается равным 0,9.

Мощность ДГУ рассчитывается по формуле:

$P_{ДГУ}$ (кВА) = $P_{ИБП}$ (кВА)×1,4 + потребление кондиционеров (кВт) / 0,7.

В данном случае 0,7 – это типичное значение cos(f) кондиционеров.

Площадь, необходимая для размещения ДГУ на прилежащей к ЦОДу территории, зависит от ее мощности (табл. 3).

Мощность ДГУ (в контейнере), кВт	Занимаемая площадь, машиноместо
До 200–300	1
300–600	2
600–1000	3

Таблица 3. Площадь, необходимая для размещения ДГУ (оценочные данные)

Целесообразность использования межрядных фреоновых кондиционеров

Как правило, при строительстве традиционного ЦОДа, рассчитанного на установку стоек мощностью 5–7 кВт, целесообразнее использовать шкафные фреоновые кондиционеры в силу существенно более низкой стоимости 1 кВт их холодопроизводительности. Но в ряде случаев приходится прибегать к альтернативным техническим решениям. К этому могут вынудить следующие обстоятельства:

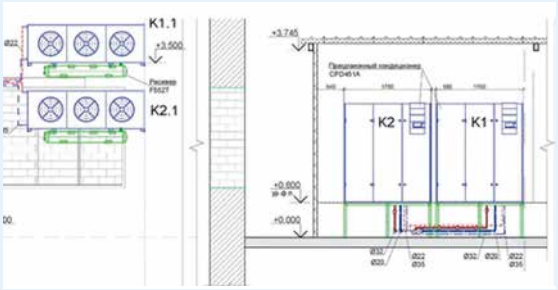
- высота помещения менее 2,8 м;
- расстояние от кондиционера до потолка меньше, чем высота фальшпола;
- тепловыделение на 1 стойку больше 8–9 кВт;
- невозможно организовать фальшпол;
- затруднен пронос оборудования системы кондиционирования (габариты самого большого межрядного кондиционера мощностью 35 кВт 0,6×2×1,2 м, в то время как габариты шкафного кондиционера (90 кВт) – 2,5×2×0,9 м).

Перед финальной (финансовой) частью статьи хотелось бы сделать несколько замечаний, которые помогут упростить оценку возможности строительства ЦОДа на обследуемой площадке.

Рассматривая систему кондиционирования, следует иметь в виду, что обычно производители рекомендуют ограничивать трассу фреоновых систем 35–40 м. На практике нередки случаи реализации систем с протяженностью трассы до 50–60 м, но при выполнении дополнительных технических условий. Ряд производителей заявляют о возможности прокладки трассы длиной до 100 м, однако примеров применения подобных экспериментальных решений в ЦОДах замечено не было. Если место установки внешних блоков системы кондиционирования находится на расстоянии 50 м от машинного зала, то нужно задуматься о переходе на чиллерные системы.

При выборе схемы резервирования основного инженерного оборудования, особенно в небольших ЦОДах, не стоит забывать о том, что порой решение 2N может оказаться дешевле решения N + 1 (или сравнимым с ним по цене), так как, например, для изготовления трех кондиционеров необходимо использовать три контроллера, три компрессора, три корпуса и т.д., а при изготовлении двух кондиционеров понадобится всего по два, хотя и большей мощности.

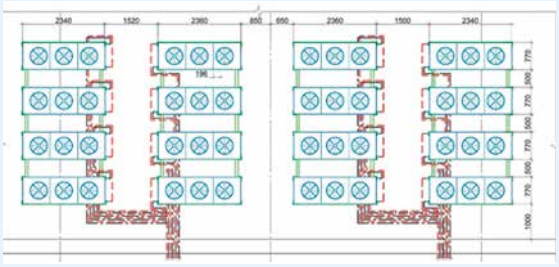
ПРИМЕР 4



Параметры площадки:

- Два кондиционера по 40 кВт
- Резервирование 2N
- Вертикальная установка
- Площадь установки с учетом сервисных зон – 9 кв. м
- Площадь ЦОДа – 28 кв. м
- Площадь внешних блоков – 32% площади ЦОДа

ПРИМЕР 5



Параметры площадки:

- Кондиционеры: 7×93 кВт + 2×40 кВт
- Резервирование N + 1
- Горизонтальная установка
- Площадь установки с учетом сервисных зон – 75 кв. м
- Площадь ЦОДа – 250 кв. м
- Площадь внешних блоков – 30% площади ЦОДа

Таблица 4. Оценка стоимости ЦОДа

Название подсистемы	Удельная стоимость
ИБП	~ $500–700 на 1 кВА
ДГУ (контейнер, шасси)	~ $300–400 на 1 кВА
Энергетика	~ $600–900 на 1 кВт мощности ИТ-систем
Кондиционеры	~ $500–700 на 1 кВт
Монтаж кондиционеров	~ $150–200 на 1 кВт
Фальшпол	~ $120–160 на 1 кв. м
АГПТ	~ $100–150 на 1 куб. м
СКУД, видео, охранная система	~ $200 на 1 кв. м машинного зала
Мониторинг	~ $500 на 1 стойку
Стойки	от $500

Оценка бюджета строительства объекта

В табл. 4 приведена удельная стоимость отдельных подсистем ЦОДа, реализованного с применением наиболее популярных технических решений.

При составлении таблицы были сделаны следующие допущения:

- вместимость ЦОДа – от 50 стоек;
- длина трассы кондиционеров – 20–30 м;
- фреоновое охлаждение;
- резервирование не выше N + 1 (ДГУ – без резервирования);
- выбор оборудования среднего ценового диапазона;
- мониторинг среднего уровня глубины.

Как отмечалось выше, стоимостные характеристики можно оценить только «в среднем по больнице», с существенными оговорками. Но даже такие оценки могут стать точкой, от которой можно будет отталкиваться при принятии решения о целесообразности строительства ЦОДа. ИКС

«Умный» холод для ЦОДа

Кирилл Дмитриев, менеджер по продукции (ИТ-охлаждение), Rittal

Для нас 2018-й – это год ИТ-инфраструктуры. Мы предоставляем широкий спектр энергоэффективных систем контроля климата, без которых инфраструктура, как известно, не может бесперебойно функционировать.

С учетом трендов

В настоящее время на повестке дня проектировщиков центров обработки данных и их заказчиков – повышение энергоэффективности и снижение энергопотребления. Поскольку системы охлаждения в ЦОДах расходуют около 40% всей электроэнергии, и заказчиками, и проектировщиками таких объектов сегодня востребованы технологии «умного» охлаждения, обеспечивающие оптимальное распределение воздушных потоков и эффективное охлаждение ИТ-оборудования.

Во всем мире у проектировщиков ЦОДов растет интерес к возобновляемым источникам энергии, а вместе с ним и желание использовать для охлаждения естественные ресурсы: либо окружающий воздух, либо геотермальные источники. Однако в России, где цены на электроэнергию ниже, чем в европейских странах, подобных проектов пока немного.

Зато в нашей стране набрал силу тренд оптимизации пространства дата-центров: площади на таких объектах стоят дорого. Применительно к системам ИТ-охлаждения этот тренд проявляется в стремлении разместить «максимум холода» в самых компактных корпусах. С другой стороны, растет количество высоконагруженных стоек (сегодня во многих проектах нагрузка на стойку превышает «классические» 7 кВт и выходит на уровень 10–20 кВт).

Руководствуясь этими трендами, мы ставим своей задачей сформировать у заказчиков новое представление о себе как о поставщике широкого спектра систем для ИТ-охлаждения и приняли решение сфокусироваться на межрядных системах. Они более предсказуемо и стабильно, чем шкафные прецизионные кондиционеры, обеспечивают холодом каждого его потребителя и именно там, где это необходимо.

Преимущества межрядного кондиционирования и предрассудки

Известно, что шкафные прецизионные кондиционеры «раздают» холодный воздух через пространство под фальшполом. Однако в этом пространстве часто размещают кабеленесущие лотки, а они создают препятствия для прохождения воздуха и могут становиться причиной возникновения встречных потоков воздуха. В результате под фальшполом могут появиться завихрения, а если расчеты при проектировании серверного зала выполнены не совсем корректно, то воздухораспределительные плитки в начале ряда стоек начнут работать на забор холодного воздуха, а в конце ряда будут выдавать его максимальный приток. Понятно, что в случае такого неравномерного распределения воздуха температурный и воздушный режимы будут далеки от оптимального.

Межрядные кондиционеры подобными «болезнями» не страдают. Им вообще не нужен фальшпол: эти системы размещаются в местах, где требуется охлаждение, – максимально близко к ИТ-оборудованию. И пусть для охлаждения ИТ-нагрузки заданной мощности таких межрядных машин потребуется больше, чем шкафных кондиционеров, зато они компактнее и позволяют экономить площадь.

К тому же при использовании межрядных систем охлаждения гораздо проще обеспечивать резервирование, переключение и поэтапное введение объекта в эксплуатацию. Если ЦОД на проектную мощность планируется выводить в течение нескольких лет, то при использовании межрядных кондиционеров можно так скомпоновать систему охлаждения, что постепенный ввод в эксплуатацию пройдет для нее без потери эффективности.

Однако, несмотря на все достоинства систем охлаждения этого типа, в России заказчики и проектировщики небольших, на 10–20 стоек дата-центров предпочитают шкафные прецизионные кондиционеры на фреоне даже в том случае, если всё – габариты помещения, компоновка системы и т.д. – говорит в пользу фреоновых межрядных систем и такое решение выглядит оптимальным.

Но недостаток оптимизма у заказчиков нас не останавливает, и мы продолжаем развивать линейку своих фреоновых систем, наращивая мощности машин в стандартных корпусах. Так, в прошлом году мы вывели на рынок межрядные кондиционеры на фреоне мощностью 20 кВт в корпусе такой же ширины, что и 12-киловаттные системы, и глубиной 1200 мм, а в этом году появятся машины мощностью 35 кВт в корпусе шириной 600 мм и глубиной 1000 мм и 1200 мм.

Водяные межрядные кондиционеры довольно часто применяются в крупных ЦОДах, владельцы и операторы которых понимают их преимущества.

В настоящее время на стадии тестирования находятся новые модели гибридных систем, в которых для повышения энергоэффективности предусмотрены и фреоновый, и водяной контур. В зимнее время они смогут работать в режиме естественного охлаждения, способствуя таким образом повышению энергоэффективности.

В погоне за энергоэффективностью

Чтобы помочь владельцам ЦОДов добиться максимальной энергоэффективности, мы акцентируем внимание проектировщиков и заказчиков на нашей компактной системе LCU (Liquid Cooling Unit). Эта сплит-система предназначена для охлаждения микроЦОДов, сейфовых решений, а также отдельных изолированных стоек. Ее концепция проста: внутренний блок, который работает по замкнутому циклу,


Компактное эффективное охлаждение

встраивается непосредственно в стойку с ИТ-оборудованием и функционирует в паре с компрессорно-конденсаторным внешним блоком, имеющим инверторное регулирование.

Несмотря на сходство внешнего блока LCU со стандартным наружным блоком бытовой сплит-системы, это решение обладает всеми качествами, необходимыми для работы в ЦОДе: LCU может снимать до 6 кВт теплопритоков с одной и даже с двух стоек. К тому же у нее есть исполнение с двумя контурами, в котором обеспечивается резервирование внешних блоков.

Прошлый год показал достаточно высокий спрос на такие системы в России. Сегодня, с появлением опции зимнего комплекта, диапазон гарантированной работы удалось расширить до –30°С, что должно повысить привлекательность данных систем для партнеров.

Большим дата-центрам достичь заданного значения PUE может помочь система LCP Hybrid, которая недавно вернулась на рынок. Этим модулем охлаждения заменяется задняя дверь в ИТ-стойке. Система, по сути, представляет собой вентилируемые двери. При этом система LCP Hybrid пассивна, не имеет в своем составе ни вентиляторов, ни электроники. И, что самое важное с точки зрения энергоэффективности, она вообще не потребляет электроэнергию, а продувается за счет попутного движения воздуха сквозь ряды стоек с ИТ-оборудованием. Вот почему система применяется в крупных ЦОДах, где таких рядов много, и неизменно показывает на подобных объектах высокие результаты.

Будущее ИТ-охлаждения = чиллер + адиабатика

Коэффициент PUE часто является аргументом выбора в пользу чиллеров: применение на объекте чиллерных систем позволяет снизить этот показатель до 1,4 и даже до еще меньших значений – за счет использования естественного охлаждения, или фрикулинга.

Все холодильные машины Rittal работают с температурным режимом хладоносителя +15/20°С, что выше, чем в промышленных климатических системах – +7/12°С. Такой подход способствует повышению общей энергоэффективности системы охлаждения. Кроме того, он позволяет начать частично использовать фрикулинг при понижении температуры наружного воздуха до +10°С, а при достижении значения +3°С переходить на естественное охлаждение полностью – отключить все основные потребляющие электроэнергию компоненты, за исключением вентиляторов и насосов. В тех регионах России, где период преобладания низких температур длительный, чиллерные системы Rittal демонстрируют высокую энергоэффективность.

Дальнейшее снижение коэффициента PUE в дата-центрах достигается благодаря подключению к охлаждению адиабатических систем, осуществляющих тонкое распыление под давлением холодной воды, которая забирает у воздуха тепловую энергию. У нас в настоящее время в разработке находится целая линейка новейших адиабатических установок, часть из которых уже задействована в проектах охлаждения ЦОДов. Более того, если у заказчика есть потребность, то мы можем интегрировать адиабатическую установку в классический чиллер. В этом случае благодаря дополнительному охлаждению воздуха за счет орошения распыляемой водой удается добиться снижения температуры воздуха на входе в холодильную машину, что существенно повышает ее эффективность.

Максимальная гибкость

Приведенный выше пример показывает, что наши возможности не ограничиваются рамками типовых решений, и мы всегда идем навстречу потребностям и интересам заказчиков, если для проекта требуется нестандартное решение в области охлаждения для ЦОДа. При этом наличие собственного производства позволяет адаптировать чиллеры, межрядные кондиционеры и другие системы Rittal к задачам конкретного проекта без внесения кардинальных изменений в их конструкцию. Таким образом драматического повышения цены не происходит, и это положительно встречается заказчиками.

Для повышения осведомленности проектировщиков и собственников ЦОДов обо всем спектре продуктов и решений компании Rittal в этом году будет запущено специализированное облачное хранилище информации (продуктовых презентаций, технической документации, чертежей) с удобной навигацией, доступ к которому будет открыт для всех желающих. Партнеры компании смогут углубить свои знания о традиционных продуктах и познакомиться с новинками в ходе обучающих вебинаров, открытых как для участия в режиме онлайн, так и для просмотра в записи на YouTube.

Новинок в области ИТ-охлаждения у нас в этом году ожидается несколько. Не раскрывая подробностей, скажем, что в наших планах представить обновленную линейку внутренних водяных блоков, а также анонсировать выход новых фреоновых машин.

Словом, следите за новостями: будет интересно.

«Озеленение» ЦОДа: фантазии и реалии

Виктор Гаврилов, технический директор, «АМДтехнологии»

Идеально «зеленый» ЦОД – это, по всей видимости, серверные стойки, которые установлены в чистом поле и запитаны от солнечных батарей, а выделяемым ими теплом подогреваются грядки с петрушкой или укропом. Есть ли предпосылки для реализации такого решения?

Для обеспечения физической безопасности оборудования, для защиты от атмосферных явлений и для комфортного пребывания обслуживающего персонала серверное оборудование предпочитают размещать в здании. Как только стойки с серверами оказываются в ограниченном пространстве машинного зала, неизбежно встает проблема отвода тепла из помещения. В отличие от стойки, расположенной в чистом поле, тепло от которой рассеивается в атмосферу, серверное оборудование в машинном зале будет нагревать помещение, поэтому мы вынуждены затрачивать дополнительную энергию на отвод теплопритоков.

Конечно, всегда можно использовать возобновляемые источники энергии – солнечные батареи или ветряные генераторы, при этом ЦОД будет оставаться «зеленым», но обойтись без механических систем для отвода тепла, к сожалению, пока не удается. По этой причине производители климатического оборудования уделяют огромное внимание разработкам энергоэффективных установок.

Зелено-дорого

Самый простой и, казалось бы, наиболее дешевый вариант отвода избытков тепла – это прямая подача наружного воздуха в помещение машинного зала без какого-либо предварительного охлаждения. Фактически наружный воздух, проходя через воздушные фильтры, подается в зону холодного коридора. Теплый воздух из зоны горячего коридора выбрасывается на улицу или используется для бытовых нужд, скажем, для отопления офисных помещений.

Если температура на улице низкая, то часть нагретого воздуха поступает в камеру смешения наружного и рециркуляционного воздуха для того, чтобы воздух, подаваемый к серверному оборудованию, не был слишком холодным и на поверхности серверных стоек не образовывался конденсат. При этом чем ниже температура наружного воздуха, тем больше тепла требуется для его нагрева перед подачей в зону холодных коридоров, и соответственно меньше тепла остается для обогрева смежных помещений. Безусловно, для собственных офисных помещений тепла будет достаточно, но если речь идет об отоплении соседнего микрорайона или тепличного хозяйства, то для бесперебойного теплоснабжения таких объектов должны быть предусмотрены дополнительные меры. По этой причине низкопотенциальное тепло, получаемое на выходе из серверов, использовать для отопления проблематично. Необходимо применять трансформаторы тепла, например тепловые насосы, а это уже дополнительные затраты, влияющие на стоимость строительства и капиталовложения на начальном этапе создания ЦОДа.

Тарифы на электроэнергию и тепло в России относительно невысоки, и срок окупаемости подобных решений может достигать 10–25 лет. При отсутствии стимулирующей законодательной базы и поддержки со стороны правительства инвестиции становятся невыгодными. Как правило, подобные проектные разработки после представления технико-коммерческого обоснования пылятся на полках.

«Теплолюбивые» ИТ

Тем не менее снижение затрат на оплату электроэнергии – хороший стимул для внедрения «зеленых» технологий. Даже если нет возможности вторичного использования тепла, любые технологии, которые приводят к сокращению затрат на эксплуатацию ЦОДа, весьма востребованы. Дополнительным катализатором развития энергоэффективных систем охлаждения является расширение допустимого температурного диапазона работы серверного оборудования. Сегодня большинство современных серверов могут устойчиво работать при 32°C или даже 35°C на входе и относительной влажности воздуха 20–80%.

Если допустимая температура воздуха на входе в сервер – 35°C или выше, то можно круглый год работать на наружном воздухе. Если мы отказываемся от охлаждения в теплый период года, то температура в зонах холодного коридора будет равна температуре наружного воздуха. Соответственно, отпадает смысл поддерживать заданную температуру, и мы приближаемся к варианту установки серверной стойки в чистом поле.

Но для того чтобы гарантировать бесперебойную работу серверного оборудования, нужно подавать такое количество наружного воздуха в зону холодных коридоров, которое требуется

для работы серверов в данный момент времени. А для того чтобы исключить переток нагретого воздуха, необходимо поддерживать небольшое избыточное давление в холодных коридорах и разряжение в горячих. В зависимости от загрузки процессора изменяются скорость вращения вентиляторов серверов и, как следствие, расход воздуха через сервер. Чем выше загрузка серверов, тем больше наружного воздуха требуется подать в машинный зал, и наоборот.

Контролируя перепад давления между холодными и горячими коридорами, мы имеем возможность загружать систему, работающую на ассимиляцию теплопритоков, пропорционально загрузке серверного оборудования. Это важно с точки зрения максимальной энергоэффективности. С одной стороны, мы обеспечиваем стабильную работу серверного оборудования, с другой – снижаем потребляемую мощность системы в целом. Контроль перепада давления между коридорами позволяет соблюдать баланс между фактической загрузкой серверного оборудования и работой механических систем, отводящих теплопритоки.

Варианты фрикулинга

Однако далеко не все серверы способны стабильно работать при температуре воздуха 35°C и выше. Но это вовсе не повод отказываться от «зеленых» технологий при строительстве ЦОДа. Конечно, трудно представить инвестора в России, который будет вкладываться в строительство ветряных генераторов для нужд собственного ЦОДа. Тем не менее для уменьшения воздействия дата-центра на окружающую среду вследствие отвода тепла от серверного оборудования существует масса возможностей, не требующих больших инвестиций. Более того, применение современных технологий позволяет значительно снизить затраты на электроэнергию, что, в свою очередь, приводит к быстрой окупаемости первоначальных вложений.

Практически у всех ведущих производителей климатических систем для ЦОДов в ассортименте выпускаемого оборудования есть отдельный модельный ряд для «зеленых» ЦОДов. Многие компании постоянно совершенствуют свою продукцию: появляются все новые модификации и поколения оборудования, нацеленного на снижение потребляемой мощности за счет использования свободного охлаждения практически в течение всего года. Расширение модельного ряда свидетельствует о том, что подобные технологии востребованы на рынке. Рост предложения приводит к постепенному снижению стоимости оборудования за счет возрастающей конкуренции, что способствует дальнейшему развитию и повышению привлекательности «зеленых» технологий для инвесторов.

В основном применяются два принципа свободного охлаждения. В первом, наиболее распространенном варианте для отвода тепла от серверного оборудования используются моноблочные установки, как правило, располагаемые рядом со зданием или на кровле. Нагретый воздух из машинного зала проходит через рекуперативный теплообменник, охлаждается наружным воздухом и подается обратно в помещение ЦОДа.

Рекуперативный теплообменник разделяет воздушные потоки, не допуская смешения внутреннего и наружного контуров, что устраняет возможность воздействия внешней атмосферы на микроклимат серверных помещений. Полностью исключается попадание пыли, осадков или задымления во внутренний контур установки. Более того, появляется возможность активно использовать в наружном контуре адиабатическое охлаждение без опасения повышения влажности воздуха в помещениях ЦОДа.

Именно применение адиабатического охлаждения дает возможность значительно экономить электроэнергию в теплый период года. В ряде случаев в зависимости от региона установки оборудования и допустимой температуры в зонах холодных коридоров удается полностью отказаться от использования холодильных машин. Если риски потери информации в результате возможного перегрева серверного оборудования слишком высоки или заказчик просто хочет подстраховаться, установку всегда можно дооснастить секцией воздухоохладителя, работающего с внешней либо встроенной холодильной машиной (рис. 1).

В любом случае алгоритм работы подобных установок нацелен на то, чтобы полностью исключить или свести к минимуму использование систем механического охлаждения. Зачастую

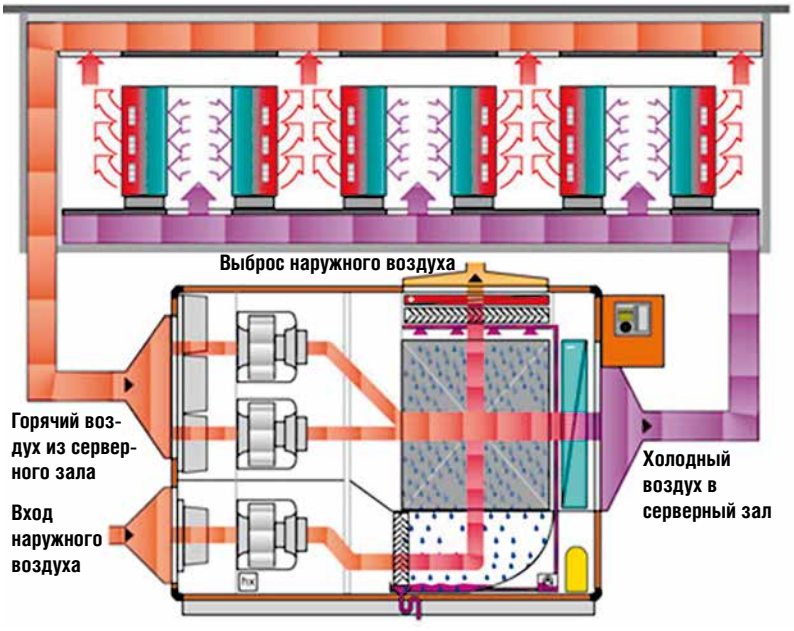


Рис. 1. Принципиальная схема работы установки с адиабатическим охлаждением и встроенной холодильной машиной

компрессионное охлаждение может действовать лишь несколько десятков часов в году, все остальное время установки работают в режиме свободного либо адиабатического охлаждения.

В зависимости от конкретного производителя типы рекуперативных теплообменников, варианты адиабатических систем и конфигурации установок могут быть различными. Как правило, производительность одной такой установки 50–300 кВт, хотя за счет модульности устройств может доходить до 500 кВт и более.

Пожалуй, один из главных недостатков этих решений – весьма внушительные размеры установок и необходимость прокладки воздуховодов большого сечения для подачи холодного воздуха в машинные залы и забора горячего воздуха для его охлаждения. Все это накладывает определенные ограничения на применение подобных систем, особенно когда речь заходит о строительстве ЦОДа в существующем здании.

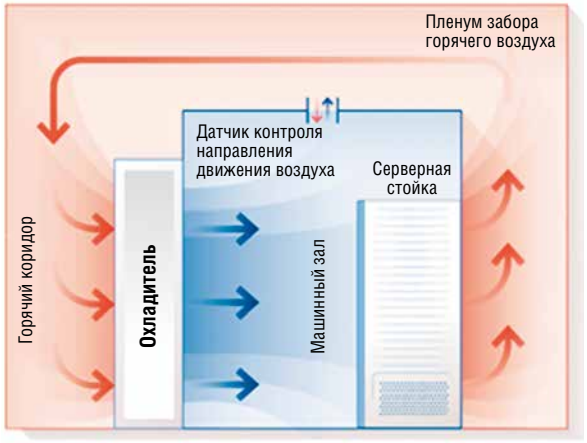


Рис. 2. Принципиальное расположение датчика, фиксирующего направление движения потока воздуха

Второй вариант, который в последнее время также становится популярным, основан на отказе от применения громоздких воздуховодов – для этих целей воздухоохладители максимально приближают к тепловой нагрузке. Как и в первом случае, время работы холодильных машин сводится к минимуму либо удается вовсе отказаться от их использования.

К данному варианту можно отнести решения с жидкостным охлаждением серверного оборудования, когда тепло отводится непосредственно от процессоров и блоков питания. Подобный подход распространяется все шире, практически любой стандартный сервер может быть дооснащен контурными тепловыми трубами. Это теплопередающее устройство, работающее по замкнутому испарительно-конденсационному циклу и использующее капиллярное давление для прокачки теплоносителя.

Такое решение избавляет от вентиляторов, установленных в сервере, а также от радиатора на центральном процессоре. Тепло отводится на внешний коллектор, по которому циркулирует теплоноситель. Температура жидкости во внешнем контуре достигает 45–50°C. Это позволяет не только отказаться от холодильных машин или затрат на воду для адиабатического охлаждения, но и вторично использовать тепло в холодный период года для отопления офисных помещений, подогрева грядок в теплицах и т.п.

Холодная стена

Более простой вариант, не требующий дополнительных затрат на строительство здания с громоздкими воздуховодами либо на модернизацию серверного оборудования, предполагает установку воздухоохладителей с большой площадью теплообменной поверхности в непосредственной близости от серверов. Это дает возможность сократить путь движения воздуха, использовать высокотемпературный теплоноситель. Такой подход, подразумевающий сдвиг парадигмы от «контроля давления» к «доступности воздуха», получил название «холодная стена». Традиционный контроль давления или температуры в холодных или горячих коридорах заменяется простым механизмом, гарантирующим достаточное количество холодного воздуха, который может забирать серверное оборудование.

Инициативы OCP и Open19

Большое влияние на повышение энергоэффективности и экономичности ЦОДов оказывает инициатива Open Compute Project (OCP). OCP предполагает создание открытых стандартов и архитектур ИТ-оборудования, нацеленных на снижение потребляемой мощности и повышение температурного диапазона работы за счет дизайна аппаратных компонентов системных плат и элементов питания. Оптимизируется расположение процессоров, памяти и жестких дисков для увеличения эффективности системы охлаждения. OCP также предусматривает разработку серверных стоек со встроенными системами бесперебойного питания и СКС.

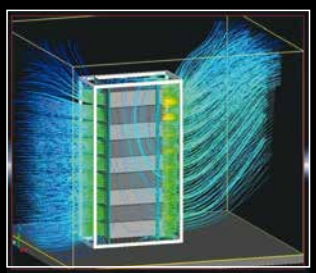
Недавно на рынке появилась новая инициатива Open19, имеющая с OCP много общего. Понятно, что участие в подобных программах – прерогатива крупных производителей и потребителей серверов, таких как Microsoft, IBM, Hewlett Packard, Cumulus Networks, «Яндекс», Facebook. Прогрессивные разработки не остаются незамеченными, и технологии, которые сегодня применяются в основном в корпоративных ЦОДах, через некоторое время распространятся повсеместно, причем не только для серверов, но и для всей инженерной инфраструктуры. Поэтому уже сейчас стоит обратить внимание на алгоритмы управления инженерными системами, задействованными в современных «зеленых» ЦОДах.

Rittal – The System.

Faster – better – everywhere.

Периферийный ЦОД Rittal – платформа для быстрого создания IT-инфраструктуры.

- Принцип ЦОД «под ключ»
- Модульность и простая расширяемость
- Все необходимые компоненты от одного поставщика
- Согласованность всех комплектующих между собой
- Наивысший уровень качества и эффективности решения в своём классе



С помощью CFD (Computational Fluid Dynamics) учитываются геометрические и термические характеристики корпуса, а также встроенные компоненты и производится визуализация на тепловой диаграмме.

Computer Multi Control III (CMC III) контролирует температуру, влажность воздуха, наличие дыма, расход энергии и доступ. Шина CAN-Bus (Controller Area Network) позволяет снизить затраты при прокладке кабеля и монтаже.

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

RITTAL

FRIEDHELM LOH GROUP

www.rittal.ru

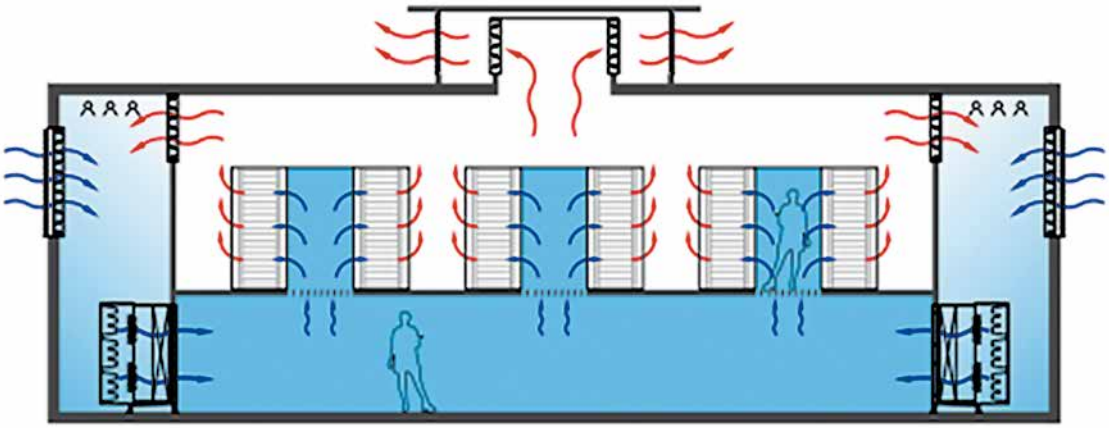


Рис. 3. Конфигурация с прямым фрикулингом

Необходимость подавать большой объем воздуха для удаления тепла от серверных стоек может привести к высокой скорости потока, особенно при неверно рассчитанном сечении воздуховодов или при заниженной высоте фальшпола. Поэтому основное внимание уделяется площади поперечного сечения всего пути движения воздушного потока, чтобы обеспечить низкую скорость воздуха. Для того чтобы соблюдать баланс между текущей тепловой нагрузкой и количеством воздуха, подаваемого в помещение, достаточно выделить холодные или горячие коридоры и контролировать направление движения потока воздуха в месте, объединяющем зоны теплого и холодного воздуха.

В машинном зале в канале между горячей и холодной частями помещения устанавливается датчик расхода воздуха (рис. 2). Воздух подается через теплообменник в помещение и забирается серверами, где поглощает тепло и через фальшпотолок отводится назад к теплообменнику. При этом машзал выполняет функцию компенсационного помещения, и обслуживающий персонал работает в комфортных условиях.

Если датчик потока фиксирует слишком большой переток холодного воздуха из холодной зоны в горячую, то реальная производительность системы кондиционирования превышает текущие тепловыделения от серверного оборудования, и наоборот. Подобный принцип управления системой охлаждения возможен при условии, что скорость движения воздушных потоков во всем пространстве машинного зала не превышает 1,5–1,8 м/с.

Применение высокопотенциального теплоносителя, например с температурным графиком 28/21°С, позволит на больший период года отказаться от использования чиллеров. Система может работать в режиме либо адиабатического охлаждения, либо свободного охлаждения только за счет низкой температуры наружного воздуха. Для серверного оборудования, способного стабильно работать при температуре воздуха в зонах холодного коридора +35°С и выше, можно и вовсе отказаться от холодильных машин.

Для дополнительной экономии электроэнергии можно организовать симбиоз между «холодной стеной» и функцией прямого воздушного фрикулинга (рис. 3).

Для реализации прямого фрикулинга потребуется только установить дополнительные воздушные клапаны для забора и выброса воздуха. В зависимости от температуры и относительной влажности наружного воздуха система может автоматически переходить в режим свободного охлаждения без включения холодильных машин. При повышении относительной влажности наружного воздуха или в случае задымления клапаны подачи и выброса наружного воздуха перекрываются, и система автоматически переходит в режим 100%-ной рециркуляции.

Россия не Голландия

На мировом рынке строительства «зеленых» центров обработки данных лидируют Нидерланды. По данным Dutch Data Center Association, в Голландии более 90% ЦОДов площадью свыше 1 тыс. кв. м активно применяют «зеленые» технологии, включая возобновляемые источники энергии, вторичное использование тепловой энергии, в том числе для отопления зданий в прилегающих районах. Это неудивительно – внедрение экологичных систем стимулируется поддержкой со стороны правительства, законодательной базой и налоговыми вычетами.

В России не меньше возможностей широкого применения «зеленых» технологий. Параметры климата, водные ресурсы, высокий профессиональный уровень инженерного персонала – хороший базис для повсеместного внедрения подобных решений. Относительно низкая стоимость электроэнергии и тепла не позволяет сегодня в полной мере использовать мировой опыт и заниматься собственными разработками. Тем не менее появляются все новые проекты, нацеленные на достижение максимальной энергетической эффективности, и интерес к ним растет с каждым годом. Это вселяет уверенность, что будущее в развитии ЦОДов принадлежит «зеленым» технологиям. ИКС

Умному городу – умную инфраструктуру

Продукция отечественной торговой марки ITK группы компаний IEK поможет выполнить задачи импортозамещения и цифровой трансформации экономики страны, считает продакт-менеджер ГК IEK Алексей Чураков.

Алексей Чураков

– С развитием цифровой экономики в России возрастают потребности в центрах обработки данных и сетевой инфраструктуре. В условиях непростой политической ситуации виден разворот в сторону российских производителей, особенно у государственных компаний. Мы все чаще сталкиваемся с ситуацией, когда заказчик хочет заменить в своем проекте продукцию известных мировых брендов качественными решениями отечественных производителей, в том числе ГК IEK.

Направление решений для ИТ-рынка в компании динамично развивается – продажи 19" шкафов и стоек в 2017 г. выросли на 190%, а наша доля рынка телекоммуникационных шкафов удвоилась. Материалы для производства у нас в основном поступают от отечественных поставщиков. Наличие собственных заводов с отлаженной системой технологического контроля позволяет тщательно контролировать качество выпускаемой продукции.

– Какие инфраструктурные решения ITK пользуются наибольшим спросом? Какие преимущества получает заказчик?

– Наибольшим спросом пользуются решения для структурированных кабельных сетей, организации серверных помещений и кроссовых зданий. На СКС торговой марки ITK мы предоставляем гарантию 25 лет при условии, что вся СКС строится на нашем оборудовании, а компания, выполняющая работы по монтажу, имеет сертификат официального инсталлятора и как минимум двух сотрудников, прошедших у нас обучение. Мы разработали большой перечень обучающих курсов разной сложности, и любой желающий может бесплатно пройти обучение через наш сайт.

Наши преимущества по сравнению с мировыми брендами – не только цена и собственные заводы в РФ, но и меньшие сроки поставки, отлаженная логистика, наличие крупных складов на территории России и возможность изготовления нестандартных изделий по индивидуальному ТЗ заказчика.

– Какие программные решения компании популярны у заказчиков?

– Мы не просто предлагаем продукт, а предоставляем обширный набор инструментов – от конфигураторов для подбора изделия по параметрам до динамических блоков для информационного моделирования, – которые помогают превратить этот продукт в готовое решение. Мы предлагаем базы оборудования для разработки проектной документации для программ Revit, AutoCAD и российской САПР-платформы nanoCAD. Конфигураторы по подбору шкафов и аксессуаров у нас связаны. Из программы подбора шкафа можно перейти в программу подбора аксессуаров для выбранного варианта шкафа.

– На какой ценовой сегмент рынка ориентирована продукция компании?

– Мы стараемся работать в среднем ценовом сегменте. Наша продукция отличается высоким качеством, которое обеспечивается за счет двойного контроля: выходного – на заводе и входного – в собственной лаборатории при поступлении готовой продукции на склады компании. На шкафы торговой марки ITK компания предоставляет гарантию три года. Если эксплуатировать изделия в соответствии с рекомендациями, указанными в паспорте, то срок их службы составит 25 лет.

– Каковы конструктивные особенности климатических шкафов наружной установки?

– Шкаф с управлением микроклиматом обеспечивает работу оборудования в заданном температурном диапазоне, а также требуемую вандало-, пыле- и влагозащиту. Мы изготавливаем корпуса со степенью защиты IP55 с комплектацией и оснасткой, которые позволяют размещать их в климатических условиях с крайне низкими температурами зимой и высокими летом. В таких корпусах используются двойные металлические стенки толщиной 2 мм, между которыми уложен утеплитель, способный противостоять морозам.

Мы предлагаем несколько вариантов охлаждения размещаемого в шкафу оборудования: работающий от электрической сети кондиционер мощностью 1,5–2,5 кВт AC, кондиционер мощностью 1,5–2,5 кВт AC/DC, адаптированный под постоянное напряжение 48 В, и более дешевые термоэлектрические кондиционеры Пельтье мощностью 0,4–0,8 кВт, работающие от постоянного напряжения 48 В.

Для уличных климатических шкафов нет жестких требований к конструктиву. Бывают разные требования к габаритам, возможно изготовление двухсекционного шкафа, причем в одной из секций можно будет размещать не 19" телекоммуникационное оборудование, а ИБП или аккумуляторы. Мы делаем такую продукцию по техническому заданию конкретного заказчика. В ТЗ указываются требуемые мощность охлаждения и тип питания.

– Как оцениваете перспективы рынка таких устройств в свете развития Edge Computing и IoT?

– Об IoT и Edge Computing пока больше говорят, проектов на рынке немного. Но мы прорабатываем решения для умного квартала на ассортименте ГК IEK. Недавно наши технические специалисты презентовали концепцию smart-квартала, в котором создается инфраструктура на базе IoT, позволяющая в едином сетевом пространстве совместно использовать сервисы, технологии и оборудование, тем самым повышая надежность и эффективность работы всей инфраструктуры и сокращая издержки ее содержания и обслуживания. Мы стараемся быть в тренде и следим за появлением новых технологий, чтобы продумать применение нашей продукции в качестве оконечного оборудования для технологий интернета вещей.

Как не получить «кота в мешке», покупая АКБ

Рынок VRLA-аккумуляторов перенасыщен. О том, как правильно выбрать поставщика этой продукции, мы беседуем с Николаем Сотсковым, руководителем компании Yellow Battery, основателем бренда YELLOW.

Николай Сотсков

– Николай, на рынке сегодня присутствует множество новых аккумуляторных марок. Насколько оправданна работа по продвижению батарей?

– Действительно, в сфере продажи промышленных свинцово-кислотных аккумуляторов так много новых поставщиков и марок, что легко запутаться. Создается впечатление, что конкурировать на этом рынке, продвигая какой-то определенный бренд, очень сложно. Это верно, но только отчасти. Если все важные параметры всех «аккумуляторных явлений» на рынке свести в одну таблицу, то такой конкурентный анализ отбросит большую часть поставщиков и марок, оставив лишь несколько самых активных, самых перспективных игроков.

– По каким основным параметрам следует оценивать батарейные бренды?

– В первую очередь необходимо понимать, что представляет собой завод, на котором изготавливается продукт. Подавляющее большинство поставляемых на российский рынок VRLA-аккумуляторов производится в Китае. При этом общественное мнение все АКБ по качеству исполнения автоматически делит на европейские и китайские. Однако китайских производителей тоже стоит разделить на несколько категорий. На территории КНР в настоящее время свинцово-кислотные аккумуляторные батареи выпускают более 700 предприятий. При такой острой конкуренции они буквально «лезут из кожи вон», чтобы получить возможность поработать на экспорт. Поэтому при любом запросе о сотрудничестве из России все они, включая маленькие сборочные цеха, безусловно, пообещают непревзойденные технические характеристики, соответствие заявленным параметрам и необходимую доработку. Могут и выдать себя за завод полного цикла, даже являясь лишь перекупщиками, охватывающими основную часть номенклатурных позиций. Для того чтобы ориентироваться в производственных площадках Китая, недостаточно сделать запрос через интернет. Работая дистанционно, вы рискуете получить некомпетентную фабрику с красивым сайтом и ничем не подкрепленными обещаниями. Только личное посещение завода и знание принципов и методик производства того или иного типа батарей может сформировать понимание, с каким заводом стоит сотрудничать стратегически.

Можно сформулировать несколько условий, без выполнения которых невозможен нормальный аккумуляторный бренд.

Во-первых, фабрика, на которой изготавливается продукт, должна быть крупным заводом полного цикла (входить в топ-10). Тут дело даже не в возможностях масштабирования, а в стабильности производства.

Во-вторых, продукция должна производиться только на одном заводе, иначе получается «сборная солянка». Мы на практике ощутили, насколько это важно. Когда поставщик работает с разными фабриками, его отдел маркетинга говорит: «Мы берем лучшее от каждого завода». Поверьте, в реальности это означает: «Мы берем от каждого завода самое дешевое, потому что выбрали стратегию демпинга». В случае с АКБ это приводит к ухудшению продукта в целом, и заказчик получает «кота в мешке». Если же используется единственная фабрика, то продукт выходит честным и стабильным, поскольку связка «завод – российский поставщик» будет гораздо серьезнее относиться к постоянному улучшению качества продукта. Мы не понаслышке знаем, что даже самые именитые игроки в нашем специфическом бизнесе позволяют себе иметь дело с низкокачественными производствами либо до предела снижают требования к качеству, изготавливая новую дешевую аккумуляторную серию.

В целом рейтинг АКБ по цене и качеству выглядит следующим образом:

1. Европейские батареи.
2. Европейские батареи, сделанные в Китае.

3. Хорошие китайские батареи.
4. Дешевые китайские батареи.
5. Батареи с заводов в Китае, которые делают аккумуляторы самого низкого качества для рынка охранно-пожарной сигнализации. Качество, которое никак не подходит для ИБП.
6. Вьетнамские батареи. Здесь брак может доходить до 20%.

Если у поставщика какой-либо известной марки вдруг появляется собственный бренд «бюджетной серии» аккумуляторов, то почти всегда это пункты 4, 5 или 6. При этом характеристики в описании поставщик подгонит под рынок, а его менеджеры будут петь новой марке дифирамбы.

В-третьих, важно состояние оборудования на заводе. Есть фабрики, которые действуют лет 40. Обычно такой солидный опыт воспринимается покупателем как плюс. Но ведь станки уже износились, а «прицел сбился», если говорить простым языком. Помните пословицу? «Старый конь борозды не испортит»? Так вот, у нее есть продолжение: «… но и глубоко не вспашет». Поэтому для получения современного, стабильного продукта нужно выбирать средний вариант. Не старое и не молодое производство.

В-четвертых, конкурентная борьба между производителями VRLA-аккумуляторов вынуждает их повышать энергоэффективность аккумуляторных пластин. Аккумуляторные технологии подразумевают применение не только свинца, но и различных комбинаций и сплавов. У каждой фабрики они свои. Могут задействоваться, например, и кальций, и сурьма. От того, насколько эффективно используются такие комбинации, зависят электрические свойства свинцовых пластин. А исследования и эксперименты в этой области требуют финансовых вливаний и наличия научного подразделения на предприятии. Если оно есть – это большой плюс.

В-пятых, следует учитывать финансовое состояние предприятия и готовность тратить деньги на обновление парка оборудования, развитие, исследования, строительство новых производственных линий и т.п. Возможно, государственная финансовая поддержка.

В-шестых, показательно наличие постоянного сотрудничества с требовательными к качеству внутренними заказчиками, например с государственными силовыми ведомствами или спецслужбами. Подчеркиваю – не с коммерческими структурами, не с мировыми производителями ИБП, партнерством с которыми так любят хвастаться российские поставщики. Это тоже важно, но мы с вами должны учитывать, что вендоры – это прежде всего коммерсанты, оптимизирующие свои решения и считающие деньги. А спецслужбам (по крайней мере в азиатских странах) важны в первую очередь качество и надежность. Производитель АКБ, преуспевающий на данном фронте, с высокой долей вероятности умеет выполнять заказы со всей ответственностью.

Вот самый минимальный набор требований к производству АКБ, и именно ими мы руководствовались, выбирая стратегического партнера для выпуска батарей под нашей маркой YELLOW.

– Немаловажно ведь и то, что представляет собой поставщик, который распространяет эту марку на рынке.

– Поставщик должен быть прежде всего честен и порядочен по отношению к своим партнерам и клиентам. А также иметь соответствующие компетенции.

– Но ведь это общепринятые вещи…

– Безусловно. Однако на рынке встречается много случаев «маркетингового блефа». Случалось ли вам видеть, как иногда и у продукции именитых поставщиков меняется срок службы? Конечно, современные достижения в области электрохимии позволяют увеличить этот параметр, но мы не раз наблюдали, как у многих поставщиков эта цифра в технических описаниях начинала ползти вверх сама по себе, без каких бы то ни было оснований, вместе с тендерными требованиями заказчика. Нужно иметь железные нервы, чтобы в таких условиях убеждать людей, что чудес не бывает и что законы химии и физики нельзя отменить тендерными требованиями даже самых богатых клиентов.

По поводу компетенций. На рынке масса поставщиков, но многие начали работать с Китаем дистанционно, не изучая предмета. Фабрик множество, заблудиться очень легко. Да и стабильность продукции без личного присутствия на производстве гарантировать невозможно. Аккумуляторы – продукт, требующий глубокого погружения в предмет, поэтому если команда поставщика много лет занимается только аккумуляторными батареями – это огромный плюс. Мы подбираем команду именно по такому принципу и видим, что это работает. Сотрудники Yellow Battery имеют 12–15-летний стаж работы только с АКБ, без отвлечения на какой-либо иной тип товара. Это позволяет выглядеть на рынке максимально компетентными в этой специфической области, и уровень доверия к бренду, конечно же, растет, мы это чувствуем.

– Как удается конкурировать по ценовым показателям при таком ответственном подходе к выбору производства и качеству?

– Сейчас на тренингах по управлению бизнесом популярна мысль о том, что доходы бизнеса должны расти быстрее, чем расходы. Должна увеличиваться «дельта», разность между этими двумя показателями. Многие владельцы популярных брендов воспринимают это так: должна расти наценка. Тем более, если марка уже популярна и «продает себя сама». Если создан массовый спрос на товар, то зачем продавать дешево? Так вот, мы избрали несколько иной путь и не гоняемся за сверхприбылью, а планомерно и последовательно отстаиваем честную цену нашего продукта. Таким образом, наши уважаемые партнеры могут получить не менее качественную продукцию по более адекватной цене. И нам кажется, что наши партнеры это ценят.

Двадцать тысяч лет под водой, или Особенности погружных систем

Александра Эрлих, сеньор-консультант, CABERO

Реализованные в разных странах проекты подтверждают состоятельность и конкурентноспособность погружных технологий на рынке охлаждения высокопроизводительных ИТ-систем.

«Еще немного, и майнинг начнет потреблять столько же электроэнергии, сколько вся промышленность Германии вместе взятая!» – писал в панике Manager Magazin в январе 2018 г. Журнал оценивал потребление майнинговых ферм в 22,5 ТВт/ч и отмечал, что одна из самых развитых в промышленном отношении стран Европы – Дания – потребляет сейчас всего лишь на 0,5 ТВт/ч больше.

Немецкий Spiegel, австрийский Der Standard, The Guardian, Digiconomist – мировые СМИ нагнетают панические настроения, оставляя за кадром тот факт, что даже эти колоссальные цифры меркнут перед потреблением классических дата-центров, не включающих в себя майнинговые фермы. В 2017 г. на их долю, по оценкам международных экспертов, пришлось от 1,5 до 2,5% общемирового энергопотребления. И весьма значительную часть этой энергии, как известно, «съедают» системы охлаждения.

Меня как производителя системных решений в области охлаждения не может не радовать старательно раздуваемый ажиотаж вокруг майнинга. Паника, пусть и искусственная, заставляет ИТ-сообщество вернуться к несправедливо забытой в кризисные времена теме: альтернативным системам охлаждения ЦОДов. А именно, к той их разновидности, которую принято называть погружными системами.

Тема погружных систем настолько стара, что заслуживает небольшого экскурса в историю.

Трансформаторное наследство

Открытое в 1831 г. английским физиком Майклом Фарадеем явление электромагнитной индукции привело к рождению трансформатора: 30 ноября 1876 г. российскому ученому Павлу Николаевичу Яблочкову был выдан патент на изобретение замечательного устройства, которым мы пользуемся до сих пор.

Обмотка тогдашних трансформаторов не выдерживала высоких температур, и практически сразу возникла новая задача: охлаждение этих устройств. Результатом многих изысканий стала система охлаждения трансформаторов погружением их в масло, впервые примененная Свинберном уже в конце 1880-х гг. Именно эта система явилась прообразом современных погружных систем, устанавливаемых в ЦОДах.

Начиная со второй половины прошлого века и до наших дней для охлаждения ИТ-оборудования в ЦОДах в таких системах использовались различные жидкости. Ученые продолжают экспериментировать с теплоносителями, и сейчас существует уже множество интересных решений, но начать хочется все-таки с классики. С масла.

Масляные системы охлаждения

Первые серверные погружные ванны, хладоносителем в которых являлось масло, пришли на рынок в начале 2000-х и предназначались они для графических ускорителей. Начиная с 2010-х гг. такими системами вплотную занялись японские производители.

Преимуществом систем на основе масла являются его диэлектрические свойства и более высокий по сравнению с воздухом коэффициент теплопередачи, позволяющий значительно уменьшить занимаемое серверной место – с одной стороны, и убрать холодильную машину из системы климатизации – с другой. По заверениям экспертов, уменьшение потребления электроэнергии в такой системе достигает 90%. Ес-

Производительность суперкомпьютера Vienna Scientific Claster 3 достигает 600 Тфлопс. При этом его энергопотребление составляет всего лишь 540 кВт, т.е. по 0,8 кВт на 1 Тфлопс. В ванны системы охлаждения этого суперкомпьютера залито 35 т парафинового масла с высоким коэффициентом теплопроводности.

ли принять во внимание факт вязкости масла и бóльшую нагрузку на насосы, становится понятно, что цифры несколько оптимистичнее реальных. Тем не менее экономия электроэнергии в любой бесчиллерной системе по сравнению с системой, использующей холодильную машину, существенна.

В Европе ЦОДы с масляными системами охлаждения появились относительно недавно. В 2014 г. был официально открыт австрийский Vienna Scientific Cluster 3 (VSC3), новый суперкомпьютер научно-исследовательского центра Венского технического университета.

Несмотря на явный успех и бесспорную энергоэффективность VSC3, даже спустя четыре года системы погружного масляного охлаждения не получили широкого распространения на европейском рынке из-за целого ряда недостатков.

Самый существенный из них – воспламеняемость масла, значительно усложняющая меры обеспечения пожаробезопасности в ЦОДе. Ученые и промышленники не прекращают изыскания, и линейка масел с точкой воспламенения 200°C и выше сегодня довольно велика, но эти масла весьма дороги. Стоимость масла – второй немаловажный фактор, негативно влияющий на популярность таких систем на рынке. Сложность проведения ремонтных и профилактических работ, связанная с необходимостью очистки рэков от масла перед осмотром, не вызывает энтузиазма у службы эксплуатации и является еще одним тормозящим фактором. И, наконец, для установки такой системы необходимо изменить сам привычный серверный рэк, как минимум удалить из него вентиляторы. Иными словами, потерять гарантию производителя.

Погружные системы на специальных жидкостях

Несмотря на то что основная идея погружать в жидкость выделяющие много тепла электрические части оборудования уходит корнями в масляное охлаждение трансформаторов, недостатки масла все время заставляют ученых обращать внимание на другие теплоносители. Здесь стоит снова сделать экскурс в историю.

Самым громким суперкомпьютерным проектом прошлого века стал Cray-1, названный по имени своего создателя, Сеймура Крэя.

Компьютер такой производительности считался революционным и пользовался колоссальным успехом. Одним из основных заказчиков стал Пентагон. Cray-1 заслужил признание даже в развитых странах Западной Европы. Выставочный экземпляр этого суперкомпьютера является одним из экспонатов Deutsches Museum в Мюнхене.

Запущенный в эксплуатацию в 1976 г. суперкомпьютер Cray-1 имел невиданную тогда производительность – 133 Мфлопс. С тепловыделением такой системы не справлялась ни одна из стандартных систем охлаждения, что заставило разработчиков обратить внимание на погружные системы. В качестве теплоносителя был выбран жидкий фреон.

Однако в конце прошлого века компьютер перестал пользоваться популярностью, в основном из-за многочисленных недостатков фреонов – их токсичности и влияния на озоновый слой. Вниманием инженерного сообщества завладели более современные системы охлаждения, а именно такие, в которых охлаждение осуществляется за счет испарения жидкости с теплообменной поверхности.

Испарительные системы

Эффект испарения делает теплообмен еще более интенсивным, значительно сокращая размеры серверных. Кроме того, по заявлениям производителей, жидкости нового поколения не воспламеняются – как минимум в рабочем диапазоне температур сервера, а также обладают относительно низкой вязкостью, что является огромным преимуществом по сравнению с большинством масел. Кроме того, эти жидкости, по заверениям тех же производителей, безопасны для людей, выгодно отличаясь от фреонов. В испарительных системах тепло забирается за счет перехода вещества из жидкого состояния в газообразное. По утверждению одного из производителей, при использовании таких систем возможен отвод до 20 кВт тепла от оборудования высотой 1U. Получается, что мощность одной стойки с оборудованием может достигать сотен киловатт.

У любой медали две стороны. Избавившись от воспламеняемости и токсичности, такая система приобрела другой существенный недостаток:

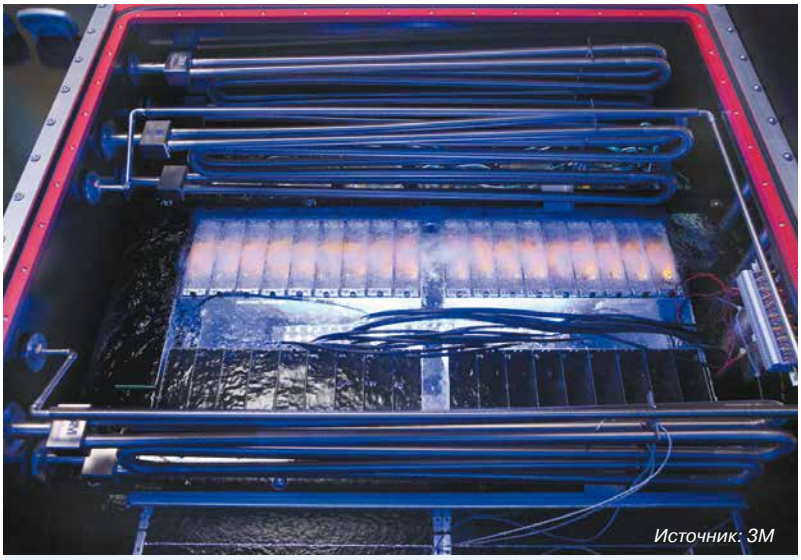
упомянутые рабочие жидкости труднодоступны. Их можно купить исключительно у производителя или авторизованных дилеров. Помимо этого жидкости активно абсорбируются материалом теплообменников, что вынуждает пользователя постоянно пополнять объем жидкости в системе.

В итоге решение получается достаточно дорогим, и не только на стадии строительства, но и на протяжении всего срока эксплуатации. ROI таких систем оставляет желать лучшего. Поэтому испарительные системы пока не получили широкого распространения.

Водяное охлаждение серверов

Вода – практически идеальный, к тому же легкодоступный хладагент. Высокий коэффициент теплопередачи, более чем в тысячу раз превышающий коэффициент теплопередачи воздуха, дешевизна и шаговая доступность делают ее желанной рабочей жидкостью для любой системы охлаждения. Если для наружных систем существенным недостатком является ее замерзание при температурах ниже 0°C, то для использования во внутренних отапливаемых помещениях это не играет никакой роли. Здесь на первый план выходит другой недостаток воды: в отличие от масла и специальных жидкостей, вода не является диэлектриком. А значит, прямой ее контакт с платой не допускается.

Несмотря на это, системы водяного охлаждения серверов применяются все шире.



Источник: 3M

В испарительных системах тепло забирается за счет перехода вещества из жидкого состояния в газообразное. По утверждению одного из производителей, при использовании таких систем возможен отвод до 20 кВт тепла от оборудования высотой 1U. Получается, что мощность одной стойки с оборудованием может достигать сотен киловатт.

В Германии сегодня очень известен проект суперкомпьютера Научно-исследовательского центра в Гархинге под Мюнхеном. Этот суперкомпьютер производительностью 3 Пфлопс получил название SuperMUC. Его идея уже не нова: на процессор «сажается» специальный водяной теплообменник, на который подается вода с температурой +40°C. Отработанная вода с температурой +70°C либо идет на отопление, либо охлаждается в климатической системе, построенной по принципу круглогодичного фрикулинга. Таким образом, холодильная машина в системе полностью отсутствует. Эта система охлаждения позволила снизить общее энергопотребление ЦОДа на 40%, а выброс углекислого газа в атмосферу на 85%. До недавнего времени SuperMUC находился на девятом месте в топ-500 суперкомпьютеров.

В России также есть замечательный проект – суперкомпьютер Научно-исследовательского вычислительного центра МГУ, построенный на аналогичной системе водяного охлаждения с круглогодичным фрикулингом. В 2015 г. компания-разработчик заслуженно получила премию Russian Data Center Awards в номинации «Комплексное решение ИТ + инженерная инфраструктура». По словам разработчиков системы, ее PUE низок до неприличия.

Несмотря на очевидные преимущества таких систем и их широкое распространение, они не лишены целого ряда существенных недостатков. Как и погружные системы, они требуют специальной доработки плат. Помимо потери гарантии производителя из-за модернизации плат, сама конструкция в силу электропроводности воды весьма сложна. А именно, в ней большое количество соединительных узлов, которые непросто контролировать на предмет

Пиковая производительность суперкомпьютера НИВЦ МГУ превышает 420 Тфлопс, при этом процессоры охлаждаются водой с температурой +45°C.

протечек. Это увеличивает как риск попадания воды на плату, так и эксплуатационные расходы. Затраты на создание таких систем также все еще слишком высоки – как в России, так и в Германии.

Дальнейшее развитие водяных систем – «холодные двери»: в дверь серверной стойки монтируется водяной теплообменник, функция которого – охлаждение проходящего через него воздуха. Все перечисленные водяные системы хороши и, безусловно, имеют будущее, но ни одна из них не является погружной, а именно они – тема данной статьи.

Условно-погружные системы

Погружать электрические части в воду без риска короткого замыкания пока не получается. Даже дистиллированная вода с высокой степенью очистки является диэлектриком лишь условно. При попадании в нее примесей (а этого в системе избежать нельзя) она с высокой степенью вероятности мгновенно начнет проводить электричество.

Именно этот факт тормозит создание полностью погружных систем на воде. Однако существуют так называемые условно-погружные водяные системы. В частности, я с 2013 г. работаю над созданием такой системы, и уже два года на базе кафедры информатики университета FH Bielefeld успешно функционирует прототип будущей системы, охлаждающий платы с графическими ускорителями.

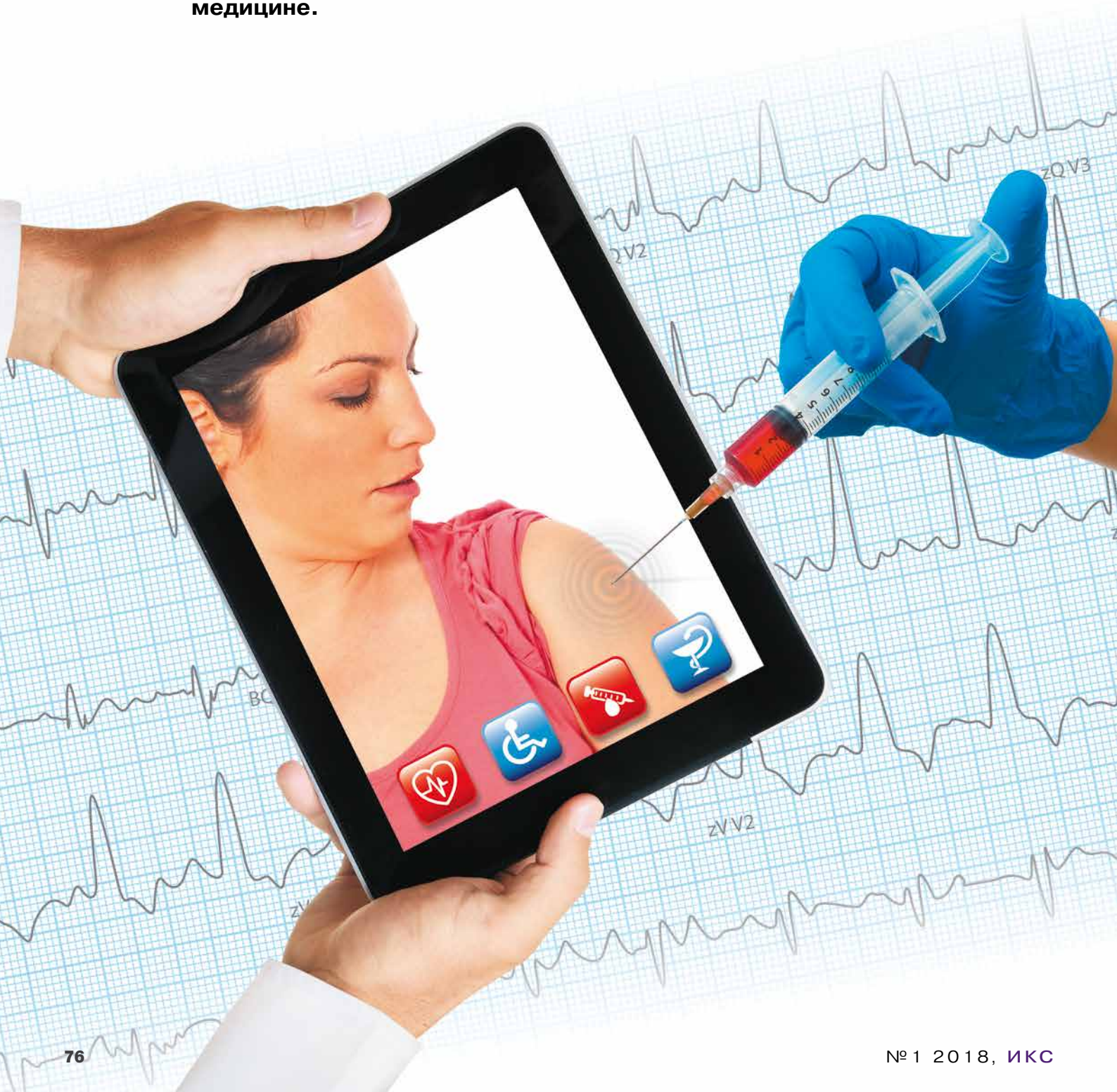
Суть системы в следующем: платы помещают в специальные кассеты, погруженные в ванну с водой. В системе отсутствует холодильная машина, вода напрямую охлаждается самосливным драйкулером, оснащенным дополнительно системой испарительного охлаждения. Единственные потребители электроэнергии в системе – это вентиляторы драйкулера, вентиляторы рэков и небольшой насос. Ванна с кассетами герметична и изолирована от окружающей среды, что снижает требования к чистоте и влажности помещения серверной до минимума. Иными словами, систему можно располагать где угодно: от специализированного ЦОДа до гаража на даче. Рэки стандартные, не требуют никакой доработки или модернизации. Вентиляторы рэков, наоборот, являются частью системы охлаждения. Потребитель может использовать любые платы, не рискуя гарантией.

Рынок не останавливается на достигнутом, и наверняка скоро появятся еще более совершенные системы с еще меньшим энергопотреблением. Там, где классическая технология охлаждения воздухом вот-вот достигнет физических пределов, именно альтернативные системы, в частности погружные, позволят вычислительной технике развиваться дальше. ИКС

Смартфон станет главным медицинским гаджетом?

Гузель Куликова

Здравоохранение готовится к оказанию медицинской помощи больным удаленно, а часть населения, осознанно относящаяся к своему здоровью, обращается к дистанционной превентивной медицине.

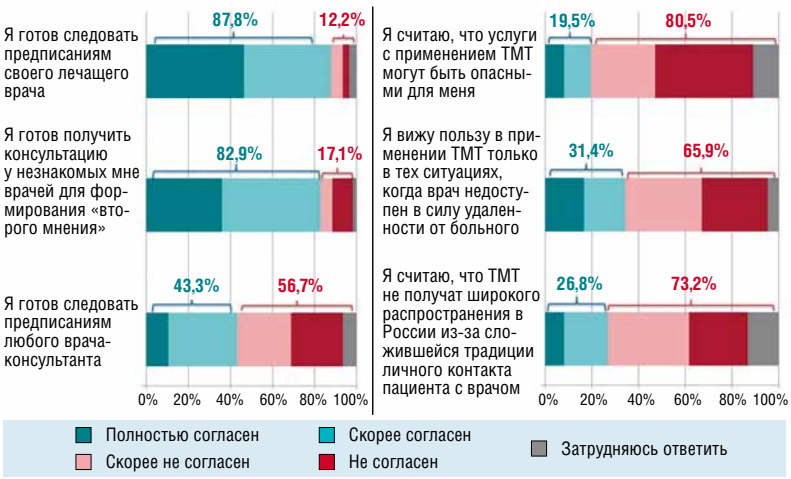


Россияне доверяют виртуальным докторам

Закон о применении телемедицинских технологий (ТМТ) в России вступил в силу с января 2018 г. Однако готовы ли россияне пользоваться услугами телемедицины? На этот вопрос попыталась дать ответ на 74-м заседании рабочей группы ИТ-специалистов медицинских организаций «Виртуальная и мобильная медицина» директор Института экономики здравоохранения НИУ «Высшая школа экономики» Лариса Попович. Она констатировала, что телекоммуникационная революция привела к беспрецедентной открытости пациентов: по данным опроса НИУ ВШЭ, в котором приняли участие около 4 тыс. медицинских работников из всех субъектов РФ, 72% россиян в возрасте 18–44 лет готовы общаться со своим лечащим врачом из дома, а не в его кабинете; 60% пациентов планируют использовать для этих целей видеосвязь посредством мобильного устройства. Со своей стороны, 81% опрошенных врачей заявили, что мобильный доступ к медицинским записям помогает координировать медицинскую помощь, 58% медработников готовы оказывать некоторые услуги удаленно, а 38% врачей уже используют электронную почту, чтобы быть все время в контакте с пациентами, имеющими хронические заболевания.

Кстати, на предложение продолжить фразу «с использованием телемедицинских технологий я готов...» 87,6% врачей ответили: «консультировать других врачей для получения "второго мнения"», 77,4% – «корректировать лечение своих пациентов с хроническими заболеваниями на основе данных мониторинга», 68,4% опрошенных готовы контролировать состояние больного с помощью носимых устройств, зарегистрированных как медицинские изделия, а 60,8% – консультировать первичных пациентов для получения «второго мнения». Корректировать тактику лечения первичных пациентов на основе данных мониторинга и медицинских документов готовы только 46,2% врачей.

В целом россияне довольно оптимистично настроены в отношении телемедицины и надеются, что внедрение современных технологий изменит ситуацию в здравоохранении к лучшему. Так, 88% респондентов считают, что использование различных форм телемедицинских технологий так или иначе повысит доступность медицинских услуг. По словам Л. Попович, результаты исследования оказались даже оптимистичнее, чем в аналогичных опросах за рубежом. Они свидетельствуют, что российские пациенты и врачи готовы к электронному взаимодействию (рис.1). Интересно, что мнения врачей и пациентов о форматах оказания телемедицинских услуг в значительной степени совпадают (рис. 2).



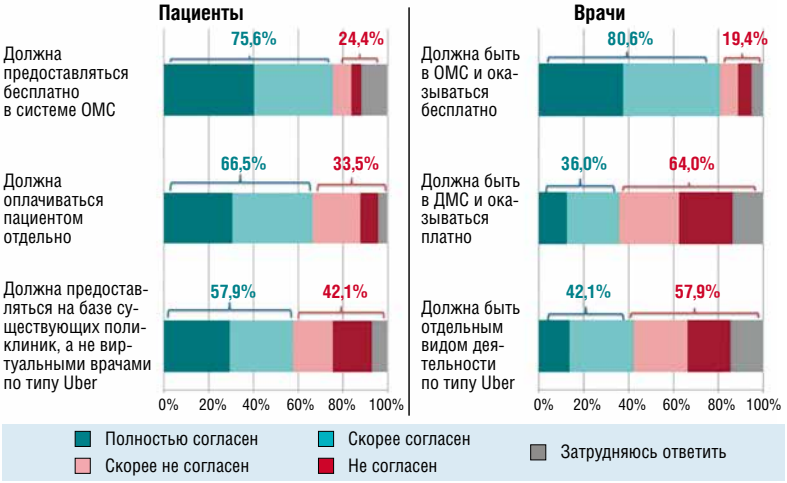
Источник: Институт экономики здравоохранения НИУ ВШЭ при содействии социальной сети «Доктор на работе»

Рис. 1. Пациенты о вариантах использования телемедицинских технологий и об ограничениях при их применении

Телемедицинские технологии должны стать повседневным инструментом прежде всего в руках семейных врачей. «Важно, чтобы человек, получивший медицинскую помощь в стационаре, находясь на амбулаторном лечении, имел возможность все время оставаться на связи со своим врачом», – заявил Борис Зингерман, руководитель направления цифровой медицины Invitro.

Как мотивировать врача использовать телемедицинские технологии? Для этого был разработан медицинский мессенджер Medsenger – SaaS-платформа, позволяющая медорганизациям и врачам предложить своим пациентам новую платную услугу: дистанционное консультирование (сопровождение, мониторинг) в промежутке между очными визитами. Главный принцип взаимодействия: пациент задает вопрос, врач отвечает, когда есть возможность. Именно это позволяет встроить новую услугу в плотный рабочий график специалиста. Фактически никакого внедрения платформы не требуется, и предварительных затрат тоже нет. Необходимо только зарегистрировать медорганизацию на данной платформе и получить доступ в свой кабинет ад-

Рис. 2. Ответы на утверждение о формате ТМТ: «Я считаю, что медицинская помощь, оказываемая с помощью телемедицинских технологий...»



Источник: Институт экономики здравоохранения НИУ ВШЭ при содействии социальной сети «Доктор на работе»

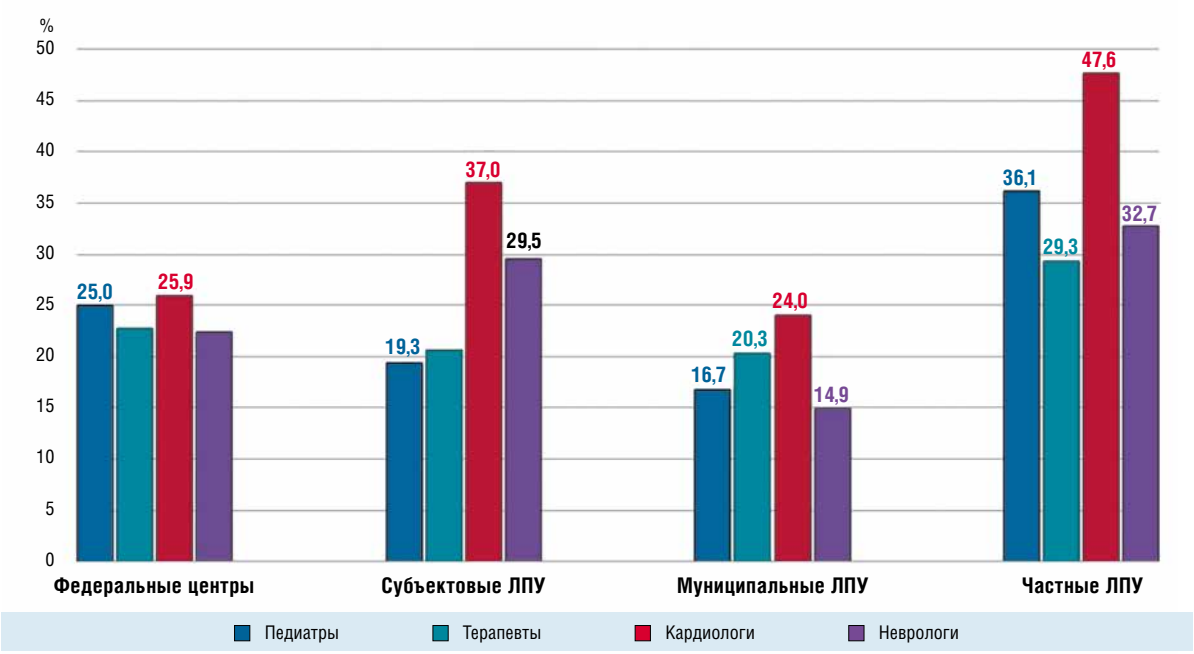


Рис. 3. Доля врачей, полностью готовых вести контроль состояния больного по данным, которые собираются с помощью носимых гаджетов, зарегистрированных как медицинские изделия

Источник: Институт экономики здравоохранения НИУ ВШЭ при содействии социальной сети «Доктор на работе

министратора. Разработанный мессенджер, как подчеркнул Б. Зингерман, полностью соответствует принятому закону о телемедицине, согласно которому консультации, включая дистанционный мониторинг и корректировку назначенного лечения, могут оказываться пациенту только лечащим врачом после установления им диагноза и назначения лечения на очном приеме.

На пути к превентивной медицине

Эксперты НИУ ВШЭ указывают, что в новых условиях врачу общей практики (персональному, семейному, офисному) отводится особая и значимая роль. Расширяя свой профессиональный функционал за счет инструментов дистанционной медицины и ИТ-ресурсов, такой специалист становится «менеджером здоровья», как для семей, так и для трудовых коллективов.

Еще в 2010 г. маркетологи отметили, что возможность получения информации из большого количества источников определенным образом отразилась на поведении потребителей. Появилась категория людей, которые на постоянной основе контролируют свое здоровье. «Есть активная часть населения, порядка 20%, которая осознанно относится к своему здоровью. В случае возникновения вопросов они обращаются к различным медицинским специалистам», – отметила Татьяна Комиссарова, декан Высшей школы маркетинга и развития бизнеса НИУ ВШЭ. Именно эта группа населения готова сфокусироваться на превентивной медицине и хотела бы иметь «единую точку входа» к медицинским услугам. Вместе с тем у 5% жителей мегаполисов, достигших среднего возраста, есть запрос на инструменты мониторинга состояния здоровья: браслеты и гаджеты, измеряющие артериальное давление, частоту сердцебиения и уровень сахара в крови. Готовность использовать показания носимых гаджетов пациентов для контроля состояния последних наиболее выражена у кардиологов (рис. 3).

К 2035 г., как сообщил Сергей Чудаков, координатор образовательных проектов направления «Превентивная медицина» в «дорожной карте» HealthNet Национальной технологической инициативы, в России планируется создать порядка 3,5 тыс. превентивных центров, использующих технологии персонализированной медицины. Основная ставка в проекте сделана на семейных врачей, планируется переподготовить порядка 50 тыс. специалистов общей практики. Для этого в 2018 г. на сетевой основе будет создан образовательный кластер – Университет персонализированной превентивной медицины, который объединит ресурсы государственных и частных участников образовательного рынка. В 2019 г. намечен старт подготовки кадров для пилотных регионов за счет смешанного финансирования: гранты – 30%, средства региональных инвесторов – 40%, средства обучающихся – 30%.

Однако внедрение ИТ в ежедневную врачебную практику затрудняется тем, что сегодня сталкиваются два поколения пользователей: «цифровые иммигранты» и «цифровые аборигены». Соответственно, как считает С. Чудаков, нужны две стратегии: в первом случае необходимо объяснять неотвратимость цифровой эпохи и научить элементарным пользовательским навыкам, во втором – прививать навыки персональной информационной безопасности и сетевой этики. ИКС

Смотреть всегда, смотреть везде

Медиаиндустрия неудержимо трансформируется. От констатации оттока телеаудитории в интернет и сетований по поводу засилья пиратов телеканалы переходят к использованию возможностей OTT, а рынок в целом даже демонстрирует успехи в борьбе с нелегальным потреблением контента.

Гузель Куликова

Новые технологии и невысокая стоимость широкополосного доступа в интернет дают россиянам возможность смотреть то, что им интересно, в удобное для них время и с доступного на данный момент устройства. И потребители этой возможностью активно пользуются. В частности, по прогнозам Аналитического центра НСК, к 2020 г. половина всех просмотров ТВ и видео будет осуществляться с мобильных гаджетов. «Потребление видео через интернет продолжает расти, будь то хостинги, стриминговые видеосервисы, онлайновые ТВ-сервисы, видеозвонки, совершаемые через мессенджеры и чаты», – констатирует аналитик iKS-Consulting Дарья Феоктистова. По данным iKS-Consulting, из числа российских интернет-пользователей 83% смотрят видеотрансляции, 82% – ТВ онлайн и 30% используют стриминговые видеосервисы.

Кинотеатры уходят в онлайн

Еще одно проявление все большего потребления видео через интернет – рост отечественного рынка онлайн-кинотеатров. Согласно исследованию РАЭК, аудитория легальных онлайн-кинотеатров увеличилась с 21,7 млн человек в 2013 г. до 39,6 млн в 2017 г.

По предварительным итогам 2017 г. объем рынка онлайн-кинотеатров составил 7,78 млрд руб. (данные iKS-Consulting). Причем если пять-шесть лет назад рынок рос в основном за счет рекламной модели, то в последние два года наиболее высокими темпами увеличивались доходы, получаемые по платной модели, заняв 59% объема рынка (4,59 млрд руб.).

Один из факторов, способствующих развитию рынка платного контента, – наблюдаемый сегодня гранулированный подход, когда пользователь приобретает, например, подписку на матчи определенной спортивной лиги или доступ к любимой передаче, премьере фильма или церемонии награждения. «Платная подписка набирает популярность, хотя принцип повсеместной оплаты контента еще не стал для большинства россиян обычным. Однако есть единицы контента, которые можно посмотреть только в онлайн-кинотеатрах, использующих исключительно платную модель», – подчеркивает Д. Феоктистова. Модель потребления «Платно, без рекламы, фильм доступен в аккаунте в любое время» в 2017 г. показала заметный рост (см. рисунок).

Стоит отметить, что самый крупный онлайн-кинотеатр – ivi.ru (34% рынка по данным iKS-Consulting) – использует обе модели оказания услуг. Иван Гринин, директор по стратегической аналитике ivi, на форуме CSTB.Telecom &

Изменение моделей потребления контента онлайн-кинотеатров

Media – 2018 сообщил, что, по предварительным подсчетам компании, в 2017 г. ее выручка по МСФО составила более 2,4 млрд руб. – рост 50% по сравнению с 2016 г. В декабре 2017 г. число платящих пользователей превысило 500 тыс., и значительная часть их – подписчики. И. Гринин говорит: «Подписка – главный тренд рынка, возможно, на долгий период времени. Но рекламная модель тоже кормит наш бизнес и помогает развиваться».

Выручка онлайн-кинотеатра Okko, работающего только по платной подписке, выросла за прошедший год на 65–67% и составила 1,25 млрд руб. В Megogo не называют конкретных цифр по выручке, однако гендиректор компании в России Виктор Чеканов пояснил, что в 2017 г. выручка от рекламной модели практически сравнялась с платной, хотя в 2016 г. данное соотношение составляло 80/20.

Главный вопрос, которым задаются топ-менеджеры всех онлайн-кинотеатров, – как увеличить свою аудиторию? Андрей Громковский, управляющий директор XX Century Fox Home Entertainment Russia, отмечает, что рынок хоть и небольшой (российская доля онлайн-видео, согласно исследованию РАЭК, в общемировом объеме составляет порядка 0,5%), но на нем уже много игроков. Поэтому важно понимать, какие изменения здесь происходят, как фрагментируется аудитория, знать предпочтения потенциальных зрителей.

Необходимо учитывать, что в стране существует большой разрыв в доходах между богатыми и бедными. «Мы через OTT-сервисы обслуживаем лишь верхушку – 15%, телеоператоры – более широкую часть аудитории. В регионах зрители не будут платить 399 руб. за новый фильм. Например, моя теща говорит: “Больше 99 руб. не заплачу”», – предупреждает А. Громковский. Для разных сегментов аудитории игроки должны разрабатывать разные продукты. Для этого нужно знать ее потребности и учитывать интересы. С точки зрения А. Громковского, пока в России не появился игрок, который создал бы продукт, востребованный миллионами людей.

Вместе с тем эксперты указывают, что при подъеме рынка происходит заметное увеличение числа игроков. Например, платный онлайн-кинотеатр намерен запустить и «Яндекс», который сейчас показывает фильмы в обмен на просмотр рекламы; появилась информация о том, что «Газпром-Медиа» планирует создавать собственный сервис для монетизации контента, произведенного холдингом. В 2018 г. конкуренция на уже консолидированном рынке онлайн-видеосервисов станет жестче.

Измерить все

Однако говорить о том, что эра вещательного телевидения канула в лету, пока рано. Валентина Удалова, директор сетей распространения программ «Первого канала», напоминает, что большая часть населения нашей страны проживает в сельской местности, где низкая платежеспособность не позволяет приобретать современные устройства и пользоваться новыми платформами. Нелинейное смотрение востребовано в больших городах с высоким уровнем занятости населения. «В крупных и некрупных промышленных городах будет развиваться линейное и нелинейное ТВ с интерактивом. А в малых населенных пунктах эфирное вещание сохранится до 2037 г., с возможностью некоторого интерактива там, где появится интернет», – считает В. Удалова.

Большое значение будет иметь измерение аудитории: вещатель должен понимать, кто его зритель и что он смотрит. Доступ к объективной информации о совокупной аудитории, которая потребляет ТВ-контент и размещенную в нем рекламу, – острый вопрос, как для телевизионщиков, так и рекламодателей. Для его решения в 2016 г. компанией Mediascope (единый телеизмеритель – бывшая TNS Russia) был реализован проект «Big TV Рейтинг», обеспечивающий измерение программного продукта на экранах телевизоров независимо от способа получения: эфир, кабель, аналог, цифра IPTV. В результате у рекламодателей появилась возможность увидеть карту потребления и суммарный рейтинг ТВ-контента.

«От измерения телевидения мы переходим к измерению total видео во всех его проявлениях. Проект "Big TV Рейтинг" – первый шаг в этом направлении», – подчеркнула Ксения Ачкасова, директор по телевизионным исследованиям Mediascope.

С 1 января 2018 г. «Big TV Рейтинг» в ежедневном коммерческом режиме предоставляет информацию о просмотре контента на экранах не только телеприемников, но и компьютеров. В проекте участвуют все желающие каналы, которые определенным образом тегируют свой контент. Система «Big TV Рейтинг» позволяет рекламодателям размешать ролики в том контенте, который распространяется в эфирных, спутниковых, кабельных каналах и в интернете. С точки зрения аналитиков, такой подход должен привести к увеличению оборотов телеканалов.

Платформу, обеспечивающую анализ зрительской аудитории и сбор информации о поведении абонентов, предлагает и компания Verimatrix. Ее решение Verspective способно определить, какой контент, в какое время смотрит пользователь, момент переключения с одного канала на другой и т.д. Эта информация дает операторам возможность использовать таргетированную рекламу, предоставлять абонентам персонализированный контент, лучше понимать интересы и запросы своих клиентов, что должно благотворно сказаться на их конкурентоспособности. Такого рода анализ может осуществляться как в системе биллинга, так и в системе просмотра видеоконтента.

Кроме того, система позволяет вести мониторинг состояния операторской сети, отслеживать состояние серверов, их функциональность, возможные угрозы. Учитывая стремление ТВ-индустрии к виртуализации видеоинфраструктуры, поставщик развернул и облачную версию своей системы – Verimatrix Secure Cloud на платформе Amazon Web Services. По словам Александра Гитина, регионального директора Verimatrix в Восточной Европе, в настоящее время стала явной тенденция перехода на такую модель операторов в Америке и в Европе, и для компании очевидно, что возможность снять с себя задачи установки, конфигурирования и управления фи-

зическим оборудованием будет положительно воспринята и в России.

Усилить контроль за распространением контента

Вслед за аудиторией в интернет мигрируют и рекламодатели. Согласно данным Ассоциации коммуникационных агентств России, по итогам трех кварталов 2017 г. сегмент интернет-рекламы увеличился на 23%, в то время как объем рекламы на телевидении вырос всего на 13%.

Однако тот контент, который смотрят россияне в интернете, производится преимущественно за счет ресурсов крупнейших отечественных телеканалов. А здесь, как и прежде, главным источником доходов является реклама. Как сообщил на форуме CSTB.Telecom & Media – 2018 заместитель гендиректора ВГТРК Дмитрий Медников, отечественные каналы производят до 97% контента исключительно за рекламные деньги, тогда как в США до 70% контента обеспечивается за счет разнообразных нелинейных сервисов и только 30% – за счет рекламных денег.

Неудивительно, что в новых условиях российские телеканалы активнее отстаивают свое право на контроль за распространением и использованием собственной продукции во всех средах ее потребления. Так, в начале текущего года НСК, «Первый канал» и компания-разработчик SPB TV заявили о коммерческом запуске технологического решения, позволяющего участникам рынка начать легальное вещание прямого эфира телеканалов в интернете с учетом правовых и коммерческих интересов производителей контента. Решение обеспечивает доступ к информации об аудитории на OTT-платформах, позволяет контролировать распространение контента и снижает уровень его нелегального использования. Телеканалы получили возможность реализовать свои рекламные возможности при вещании в интернете без технических задержек и дополнительного трафика.

OTT может открыть для телеканалов новые перспективы. Как считает Алексей Волин, заместитель министра связи и массовых коммуникаций РФ, здесь многое зависит от того, каким образом ТВ-каналы будут выстраивать свои платформы по легальному распространению данных сервисов. Вместе с тем он обратил внимание, что в прошлом году потребление OTT-видео выросло на 70–80%. Именно эта технология формирует «глобальный телевизионный роуминг», когда аудитория не только расширяется за счет эфирного вещания, но и «растет worldwide». По словам замминистра, российские производители контента могут теперь выходить на зарубежные рынки и предлагать свои услуги в любой точке мира, где есть доступ в интернет.

Скромные, но успехи

Важную роль в развитии транзакционной модели сыграла борьба с пиратством. Регуляторные меры по борьбе с нелегальным распространением контента постепенно приносят плоды: за последние три месяца 2017 г. число посетителей пиратских сайтов, по оценкам ассоциации «Интернет-видео», уменьшилось в 1,5 раза. При этом законы, регламентирующие ту или иную сферу в интернете, влияют на развитие бизнеса гораздо сильнее, чем экономические и социальные факторы, убежден генеральный директор ассоциации «Интернет-видео» Алексей Бырдин.

1 июля 2017 г. вступил в силу закон об аудиовизуальных сервисах, регулирующий деятельность онлайн-кинотеатров и других OTT-платформ. Стоит отметить, что часть подзаконных актов еще не принята и этот фактор тормозит применение закона. Согласно документу, видеосервисы, которые в сутки посещают более 100 тыс. пользователей, должны встать на учет в Роскомнадзоре и следовать ряду ограничений. Закон не распространяется на социальные сети, поисковики, видеосервисы YouTube и другие, на которых размещается преимущественно пользовательский контент. Вместе с тем участники рынка надеются, что этот закон станет дополнительным инструментом для борьбы с пиратством в интернете.

Среди регулирующих документов специалисты особо выделяют закон «о зеркалах», вступивший в силу 1 октября 2017 г. В нем прописана процедура принятия Минкомсвязью решения о признании сайта копией заблокированного сайта. Право инициировать процедуру блокировки получили федеральные органы исполнительной власти и правообладатели. «Закон реально работает, – заявил на форуме CSTB А. Бырдин. – Срок блокировки конкретного домена сократился с полугода до 24 часов: это фантастический апгрейд системы». Именно этот закон окажет позитивное действие на все отрасли, связанные с дистрибуцией контента, и приведет к росту доходов легальных сервисов, уверены в ассоциации «Интернет-видео».

В ассоциации подсчитали, как с октября по декабрь прошлого года изменилось количество посетителей входящих в топ-100 видеосайтов в России, из которых лишь два сервиса предоставляют легальный контент. «В октябре число уникальных посетителей пиратских сайтов составляло 155 млн человек, легальные сервисы ivi, Megogo набрали 20 млн», – рассказал гендиректор ассоциации. В ноябре на пиратских сайтах было зафиксировано 116 млн пользователей, тогда как число клиентов легальных видеосервисов выросло до 22 млн, в декабре соответственно пиратским контентом воспользовалось 97 млн, а услугами ivi, Megogo – 24,5 млн чел. Стоит отметить, что драйверами роста стали как усилия легальных игроков, направленные на продвижение своих сервисов и способствующие росту их качества и узнаваемости, так и укрепление правовой базы и ужесточение борьбы с пиратством.

■ ■ ■

Впрочем, само наличие нелегально распространяемого контента (по оценке iKS-Consulting, только 14% зрителей не пользуется нелегальными ресурсами), укрепляет стремление игроков медиарынка идти навстречу потребителю, предоставлять ему возможность смотреть то, что он хочет, и так, как он хочет, и развивать технологии, которые повышают его удовлетворенность. ИКС

DDoS: цели, методы, средства защиты

Сергей Орлов,
независимый эксперт

От распределенных атак «отказ в обслуживании» сегодня не застрахована ни одна организация, присутствующая в интернете. Как правило, такие атаки направлены на вывод из строя критически важных приложений и ресурсов.

По данным отчета Verizon, в мире от атак DDoS (Distributed Denial of Service) больше всего страдает индустрия развлечений, профессиональные ассоциации, сфера образования, ИТ, ритейл. Однако список потенциальных жертв включает компании и организации практически из всех отраслей. Следствием DDoS-атаки из-за медленной работы или полной недоступности сайта может стать потеря клиентов или репутации бизнеса.

Цели

DDoS-атака – распределенное нападение на ИТ-систему организации с целью довести ее до отказа. На систему направляется огромное количество запросов, из-за которых ее производительность снижается вплоть до полного «зависания». Уязвимые элементы – интернет-каналы, серверы, межсетевые экраны. Обычно для атаки используются скомпрометированные системы.

Задача атакующих – вывести сайт из строя или «под шумок» украсть данные. Часто DDoS-атаки чередуются с попытками взлома сайтов. Нередко атаки заказывают конкуренты. Другая цель – вымогательство путем шантажа. Иногда для получения выкупа прибегают к угрозам совершения DDoS-атаки. Как отмечают в Ponemon Institute, DDoS-атаки все чаще становятся основной причиной незапланированных простоев ЦОДов во всем мире.

Методы

Средняя мощность DDoS-атак в последние годы выросла до нескольких сотен гигабайт в секунду. Увеличивается число DDoS-атак с использованием сразу нескольких уязвимостей (многовекторные атаки и атаки смешанного типа). По данным Arbor Networks, многовекторные атаки составляют порядка 27% общего числа атак DDoS.

Свыше половины случаев – это DDoS-атаки с пятью и более векторами. Комплексные атаки могут быть направлены сразу на несколько сетевых уровней и элементов инфраструктуры. Например, DDoS-атаки на канальный уровень (L2) часто сопровождают атаки на уровень приложений (L7). Такие атаки могут быть очень эффективными.

DDoS-атаки с применением доступных автоматизированных инструментов и сервисов практически не требуют специальных знаний. Онлайн-сервисы нередко предлагают желающим протестировать свой сайт «под нагрузкой», но их услуги могут использоваться и для атак. С помощью автоматизированных инструментов отправляются запросы, имитирующие результат обычных действий пользователей. Такие атаки L7 имеют тяжелые последствия и трудно распознаются.

Распространенные типы DDoS-атак

Название атаки	Уровень OSI	Принцип атаки
ICMP Flood (Ping Flood)	L3	Массовая отправка пакетов, подразумевающих ответ жертвы
IP Packet Fragment Attack	L3	Отправка IP-пакетов, ссылающихся на другие пакеты, которые никогда не будут отправлены; в результате память атакуемой системы исчерпывается
Smurf	L3	По адресу широковещательной рассылки отправляется поддельный пакет ICMP Echo, адрес источника пакета заменяется адресом жертвы. Так как пакет Echo посылается по широковещательному адресу, все компьютеры возвращают свои ответы атакуемой системе. Таким образом DDoS-атаку можно усилить в сотни раз
IGMP Flood	L3	Массовая рассылка IGMP-пакетов
Ping of Death	L3	Отправка ICMP-пакетов, которые используют ошибку реализации в определенных операционных системах
TCP SYN Flood	L4	Массовая отправка запросов TCP-соединений
TCP Spoofed SYN Flood	L4	Массовая отправка запросов TCP-соединений. На каждый входящий пакет SYN система резервирует ресурсы в памяти, генерирует ответ SYN + ACK, осуществляет поиск в таблицах сессий и т.д. Цель атаки – исчерпать ресурсы системы, что происходит при потоке 100–500 тыс. пакетов SYN Flood в секунду
TCP SYN ACK Reflection Flood	L4	Массовая отправка запросов TCP-соединений на большое количество машин. Полоса пропускания жертвы будет насыщена ответами на эти запросы
TCP ACK Flood	L4	Массовая отправка TCP ACK
TCP Fragmented	L4	Массовая отправка сегментов TCP со ссылкой на другие сегменты, которые никогда не будут отправлены, что насыщает память жертвы
UDP Flood	L4	Массовая рассылка пакетов UDP (не требует предварительного установления соединения). Злоумышленники атакуют порты сервера, отсылая большое количество пакетов данных. Целевая система проверяет, используется ли порт, на который приходит пакет, каким-либо приложением, и не справляется с задачей
UDP Fragment Flood	L4	Отправка большого числа фрагментированных пакетов UDP, с которыми система также не справляется: на их анализ и сборку приходится выделять ресурсы
DNS Amplification	L7	Массовая отправка DNS-запросов с исходным адресом жертвы большому количеству легитимных серверов. На сервер, содержащий уязвимость, отправляется запрос, который этим сервером многократно тиражируется и направляется на сайт жертвы. В качестве серверов, участвующих в таких атаках, могут использоваться DNS-, NTP-, SSDP-серверы и др.
DNS Flood	L7	Атака DNS-сервера путем массовой отправки запросов
HTTP(S) GET/ POST Flood	L7	Атака веб-сервера путем массовой отправки запросов
DDoS DNS	L7	Атака на инфраструктуру DNS с помощью массовой отправки запросов

Источник: OVH

При DDoS-атаке с использованием ботнетов злоумышленники контролируют множество систем-«зомби» для создания значительной нагрузки на атакуемый сайт. Обычно прибегают к наиболее ресурсоемким запросам.

В последнее время участились атаки на IoT-устройства с целью их захвата и включения в ботнет для проведения DDoS-атак. По мнению экспертов, IoT-ботнеты станут одной из главных угроз в киберпространстве, поскольку большинство устройств IoT легко взломать, а отслеживать и анализировать осуществляемые через них атаки крайне сложно.

Число устройств, участвующих в подобных атаках, может достигать сотен тысяч. Уже есть примеры, когда пиковая мощность атак с применением данной технологии превышала 1 Тбит/с. Атаки, в которых были задействованы интернет-видеокамеры и бытовые маршрутизаторы, отмечались и в России. Пока количество атак с использованием устройств IoT невелико, поскольку таких устройств еще относительно немного.

По информации «Лаборатории Касперского», в III квартале 2017 г. увеличилась доля атак SYN-DDoS – с 53,3 до 60,4%. При этом доля TCP-атак упала с 18,2 до 11,2%, однако они по-прежнему на втором месте. Более редкими стали также атаки с использованием UDP: их доля сократилась с 11,9 до 10,2%. Уменьшилось и количество ICMP-атак – с 9,4 до 7,1%. А вот доля HTTP-атак выросла с 7,3 до 11,6%, и они вышли на третье место.

В числе особенностей текущей ситуации аналитики выделяют учащение атак на ICO-платформы и увеличение доли многокомпонентных атак, состоящих из различных комбинаций SYN, TCP Connect, HTTP Flood и UDP Flood.

Стратегия защиты

Правильная стратегия защиты от DDoS-атак поможет подготовиться к атаке и минимизировать ее последствия, снизить финансовые и репутационные риски. Меры следует принимать уже при конфигурировании сети, запуске серверов и развертывании ПО, причем последующие изменения не должны повышать уязвимость системы. При разработке приложений рекомендуется следовать стандартам безопасного кодирования и тщательно тестировать ПО, чтобы избежать типовых ошибок и уязвимостей. При обновлении программного обеспечения (а оно должно быть своевременным) всегда нужно иметь возможность «отката» на случай, если что-то пойдет не так. Планы аварийного восстановления должны также предусматривать способы устранения последствий DDoS-атак.

Защиту от атак UDP Fragment Flood обеспечивают системы глубокого анализа трафика, фильтруя «лишние» протоколы или ограничивая их по полосе. Чтобы предотвратить усиление атаки типа Smurf, рекомендуется запретить широковещательную рассылку на граничных маршрутизаторах и установить в ОС режим отбрасывания широковещательных эхо-пакетов ICMP. Для защиты от ботнет-атак применяются различные поведенческие стратегии, позволяющие выявлять нетипичные отклонения и всплески трафика.

Все устройства, подключенные к интернету, потенциально могут стать частью инфраструктуры злоумышленников и использоваться в DDoS-атаках. Чтобы минимизировать риск от устройств IoT, необходимо отключить неиспользуемые сетевые функции, вместо доступа по Telnet задействовать SSH и по возможности перейти на проводное соединение вместо Wi-Fi.

Выстраивать защиту от DDoS следует на всех уровнях. Например, для обеспечения доступности сайта можно пропускать трафик через сеть очистки, организовать защиту сайта на транспортном и сетевом уровнях, где происходят фильтрация и анализ входящего трафика, блокировка IP-адресов. Одновременное использование разнопрофильных средств защиты, включающих защиту от DDoS и от атак на приложения, а также средства мониторинга, поможет эффективно противостоять злоумышленникам.

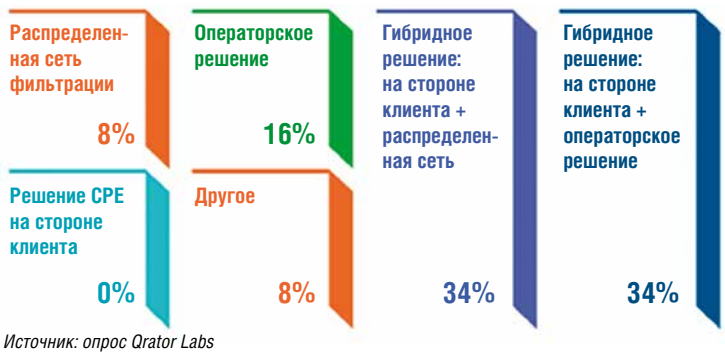
Защита от DDoS-атак на уровне приложений требует быстрой реакции на изменение вектора атаки, для чего служат автоматизированные системы, в том числе работающие на основе алгоритмов машинного обучения.

Для противодействия сложным, комплексным DDoS-атакам необходимо использовать профессиональные решения или сервисы. Если владелец ЦОДа не обладает достаточным опытом и специальными техническими средствами, DDoS-атака может привести к недоступности его сетевых устройств и ИТ-инфраструктуры клиентов.

Для мониторинга трафика можно использовать Web Application Firewall (WAF). Такой межсетевой экран способен выявлять атаки по хранимым шаблонам и распознавать необычное поведение. Можно воспользоваться облачными сервисами WAF.

Собственные аппаратные средства защиты от DDoS-атак не только недешевы, но и не всегда

Рис. 1. Наиболее эффективные решения для защиты от DDoS-атак



Источник: опрос Qrator Labs

эффективны. Согласно результатам опроса, проведенного компанией Qrator Labs в 2017 г. (рис. 1), почти 2/3 респондентов считают самым эффективным средством противодействия DDoS гибридные решения. В них система на стороне клиента (CPE) работает в сочетании с операторским решением либо использует распределенную сеть. В последнем случае «мусорный» трафик, способный вызвать перегрузку канала и недоступность сайта, проходит через распределенные центры фильтрации, где и отсекается.

Гибридный подход, совмещающий очистку трафика на уровне провайдера для отсечения лавинообразных атак и решение для защиты на стороне конечного заказчика, считается оптимальным при защите от DDoS. Поэтому растет число компаний, передающих трафик внешнему поставщику услуг (рис. 2).

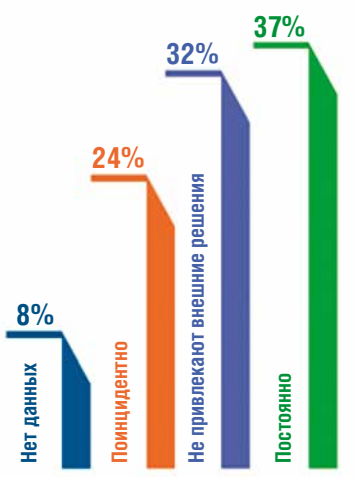
Услуги по защите от DDoS предоставляют операторы связи, интернет-провайдеры и другие компании: они осуществляют мониторинг трафика в реальном времени для отслеживания аномалий и всплесков загруженности полосы, реализуют защитные функции, которые позволяют скрыть оборудование клиента от злоумышленников, запретив к нему доступ из интернета, применяют интеллектуальные и даже самообучающиеся системы.

Защита от DDoS «по требованию» – хорошее дополнение собственных систем. Такую услугу можно включать в экстренной ситуации либо постоянно находиться под защитой, используя операторские или облачные сервисы очистки трафика.

В последние годы получило развитие еще одно интересное направление – защита от DDoS с использованием облачной аналитики больших данных. Соответствующие решения способны постоянно отфильтровывать гигабайты мусорных пакетов, доставляя каждый запрос от легитимных пользователей на целевой сервер. Алгоритмы машинного обучения позволяют действовать более интеллектуально, выявляя релевантные IP-адреса получателей, осуществляя мониторинг аномального трафика для обнаружения атак.

По данным Business Application Research Center, пока только порядка 20% компаний используют сервисы обнаружения кибератак, основанные на аналитике больших данных и контекстном анализе, но более половины из них считают, что подобный подход дает серьезные бизнес-преимущества.

Сервисы защиты от DDoS предоставляют подавляющее большинство российских провайдеров, а также многие хостинг-провайдеры: анализ сетевого трафика производится в режиме 24/7 и защита нередко способна выдержать мощные атаки – до 1500 Гбит/с. Поставщики таких сервисов обладают достаточными ресурсами и компетенцией, чтобы предложить различные решения для защиты данных клиентов, организации безопасного доступа и предотвращения атак. Результатом будет своевременное обнаружение и предотвращение DDoS-атак, непрерывное функционирование сайта и его постоянная доступность для пользователей, минимизация финансовых и репутационных потерь вследствие простоя интернет-ресурса.

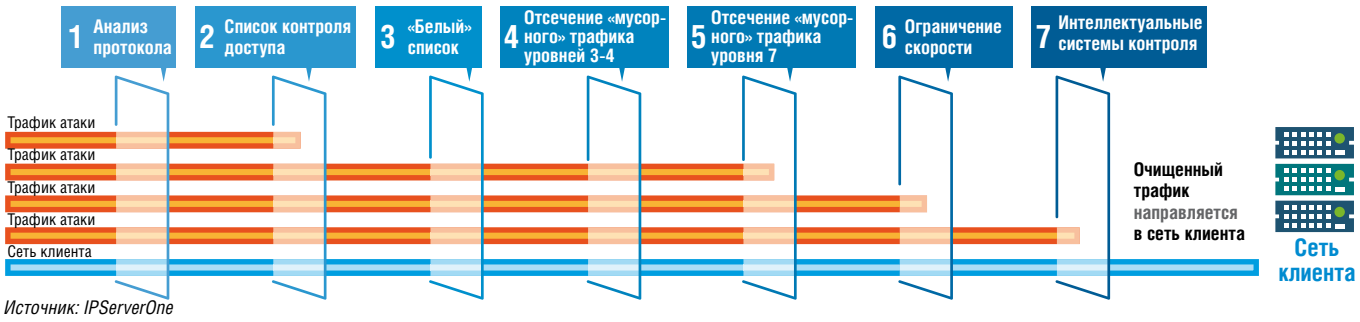


Источник: опрос Qrator Labs

Рис. 2. Частота использования сторонних решений для пропуска трафика с целью защиты от атак

Современные защитные решения обеспечивают мониторинг трафика, его фильтрацию, способствуют обнаружению сетевых атак различного типа (рис. 3). Они очищают трафик от паразитных пакетов, не препятствуя доступу легитимных пользователей, отслеживают наличие аномалий, а в случае их выявления информируют клиента о возможной DDoS-атаке. Использование подобного программно-аппаратного комплекса позволяет оператору связи или владельцу ЦОДа поддерживать качество предоставляемых услуг, непрерывность бизнес-процессов, а также снизить риски для клиентов.

Особенно эффективны (но и дороги) системы распределенной защиты. Соответствующее оборудование устанавливается у магистральных операторов, и если анализатор атак фиксирует нападение на защищаемый сайт или сервер, он моментально транслирует адреса атакующих хостов другим узлам по всей сети, и сеть начинает работать против атакующих хостов. Атака гасится, а то, что доходит до цели, отбивается фильтрами. Подобная система способна отразить атаки большой мощности. ИКС



Источник: IPServerOne

Рис. 3. Многоуровневая защита от атак при предоставлении клиентам сервиса «анти-DDoS»

Блокчейн – новый рынок информационной безопасности

Николай Носов

Рост популярности технологий распределенного реестра приводит к созданию нового рынка услуг.

In Code we trust – такой девиз характеризует наиболее последовательных сторонников использования технологий распределенного реестра и криптовалют. Убрать армию посредников, обеспечивающих доверие, и заменить их программным кодом. Успешный пример блокчейна Bitcoin показывает, что это реально. Цепочка блоков, работающая в максимально недоверенной, а часто и преступной среде, не была взломана за девять лет успешной работы. Но даже такая надежная технология не решила всех проблем* информационной безопасности. Злоумышленники атаковали менее защищенные участки технологической цепи – кошельки пользователей и криптобиржи, так что работы у специалистов по расследованию инцидентов безопасности хватало. Резкий всплеск интереса к криптовалютам в прошлом году только обострил существующие проблемы.

Уязвимости методов консенсуса

Технология распределенного реестра базируется на понятии консенсуса – механизма синхронизации данных распределенных узлов сети. В системе постоянно формируются альтернативные цепочки блоков, что является совершенно нормальным, ведь разные майнеры, конкурирующие за премию за формирование нового блока, могут почти одновременно приходить к правильному решению. Механизм консенсуса позволяет выбрать основную цепочку – определить победителя Bi + 2 (1) и отбросить альтернативные цепочки Bi + 2 (2) и Bi + 1 (3) (рис. 1).

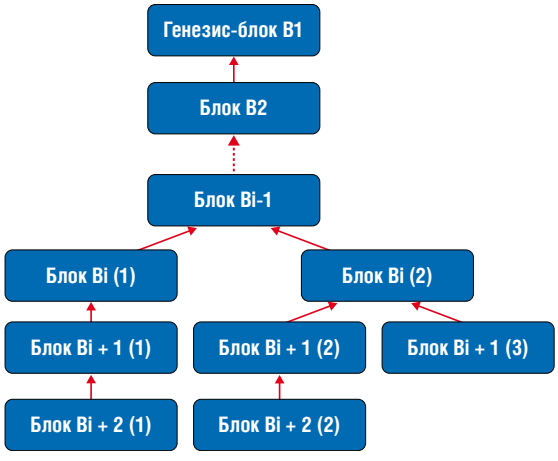


Рис. 1. Ветвление цепочки блоков блокчейн-цепи

В блокчейн-системах, использующих метод консенсуса Proof-of-work (PoW), очередной блок подтверждается участником (майнером), который первым выполнил сложную вычислительную задачу подбора хеш-функции блока в соответствии с заданными в системе условиями. Например, в Bitcoin требуется подобрать такое значение поля nonce, чтобы хеш-функция содержимого нового блока и хеша предыдущего (таким образом новый блок подвязывается к существующей цепочке) имела в первых полях заданное системой количество нулей** (значение меньше числа, определяющего сложность расчета).

В сети Bitcoin половина узлов получает информацию о новом блоке за 12 секунд. Разрыв во времени между лидерами может быть небольшим по сравнению со временем распространения информации о новом блоке. Майнер, пославший решенный блок Bi (1) первым, успеет получить поддержку большего числа узлов (нод) пиринговой сети (узел получает решенный блок и передает его дальше). Тем не менее есть вероятность появления альтернативной цепочки (форка) в узлах, первыми получивших решение другого майнера – Bi (2). Вероятность решения следующего блока Bi+1 (1) будет выше у майнеров первой группы – получив решение блока Bi (1), они сразу приступают к поиску решения Bi + 1 (1), – и сторонников первой ветки станет еще больше. При этом цепочки могут и дальше делиться, так на рис. 1 вторая цепочка блоков разделилась на Bi + 1 (2) и решенный чуть позже блок Bi + 1 (3).

Вероятность получения поддержки узлов у Bi + 1 (3) совсем мала, поэтому на следующем этапе конкурировать будут блоки более длинных цепей Bi + 2 (1) и Bi + 2 (2), причем у Bi+2 (1) шансов на победу будет больше. В результате такого итерационного механизма узлы приходят к консенсусу, и данные в них синхронизируются. Считается, что в блокчейне Bitcoin консенсус гарантированно достигается через шесть решенных блоков.

Для быстрого расчета нужны большие вычислительные мощности. Альтернативный вариант – использование метода Proof-of-stake (PoS). Тогда вероятность формирования участником очередного блока пропорциональна доле, кото-

* Блокчейн: технология не решает проблему доверия. «ИКС» № 3–4'2017, с. 66, № 5–6'2017, с. 69.

** Блокчейн и облака. «ИКС» № 3–4'2016, с. 48.

рую составляют принадлежащие этому участнику расчетные единицы данной криптовалюты. Идея привлекательна и понятна – отказаться от майнинга за счет вероятностного подхода, при этом давать предпочтение участникам, наиболее заинтересованным в правильном функционировании системы.

Однако огромное количество электричества использующими PoW блокчейнами сжигается не зря – именно за счет произведенной работы, привязки к физическому миру повышается устойчивость к ряду возможных атак (табл. 1). Например, при так называемой атаке Сибиллы, когда новичок сети окружается фейковыми узлами злоумышленника, который ставит его под свой контроль, жертве достаточно связаться с одним «правильным» узлом сети PoW, чтобы разобраться в ситуации. Ведь мощности, затраченные на построение «правильной» длинной цепочки блоков, просто недоступны злоумышленнику.

Сжигаемое электричество препятствует проведению и «атаки издалека», которой тоже может быть подвержен блокчейн, использующий консенсус PoS. Ведь при отсутствии дополнительных ограничений злоумышленник может построить свой альтернативный блокчейн прямо с генезис-блока и затем выдать его за правильный. То же затраченное электричество делает невыгодными краткосрочные атаки («атаки взятками»), когда злоумышленник платит за товар, получает его, а потом объявляет вознаграждение за строительство усеченного блокчейна с блока, не включающего его платеж.

В своей «Белой книге биткойна» Сатоши Накомото писал: «Если какой-то жадный злоумышленник сможет собрать больше процессорных мощностей, чем есть у всех честных узлов, ему придется выбирать между тем, чтобы с их помощью обманывать людей и красть их платежи либо атаковать сеть иным образом, и тем, чтобы создавать новые денежные единицы, используя свои мощности. Гораздо выгодней для него стало бы играть по правилам, которые поощряли бы его большим количеством новых денег, чем у всех остальных, нежели наносить вред системе и таким образом и его собственному благосостоянию».

В открытых блокчейнах, основанных на PoW, такой подход работает. Теоретически возможная атака «51 процент», когда злоумышленник задействует более половины мощности сети (в действительности есть вероятность успешной атаки и при меньшей контролируемой мощности), так и остается гипотетической. Риски ее успешного проведения увеличиваются для альтчейнов с низким хешрейтом (т.е. вычислительной мощностью) сети.

А вот в простейших вариантах PoS-консенсуса наиболее экономически выгодным поведением может быть размножение ответвлений цепочки

Тип атаки	Метод консенсуса		
	PoW	PoS	DPoS
Отказ в обслуживании	Есть	Есть	Есть
Атака Сибиллы	Нет	Есть	Есть
Атака издалека	Нет	Есть	Есть
Краткосрочная атака	Нет	Есть	Нет
Атака предвычислением	Нет	Есть	Нет

Таблица 1. Уязвимость методов консенсуса для различных типов атак

(форков) блока для повторной траты средств (атака double-spending). Ничем особенно не рискует при PoS-консенсусе и проводящий «атаку предвычислением», когда злоумышленник добавляет транзакцию в блок Bi (2) так, чтобы иметь возможность решить следующий блок Bi + 1 (2). Атакующий может строить свою цепочку в секрете, чтобы потом обогнать правильный блокчейн с транзакцией, которую хочет отменить. В борьбе с такими махинациями помогают более сложные алгоритмы доказательств доли (DPoS, deposit based proof of stake), в которых используется залог, конфискуемый в случае некорректного поведения участника.

Общей проблемой для всех видов консенсуса является атака «отказ в облуживании», или DoS, когда злоумышленник наполняет сеть транзакциями малой стоимости. Такая атака на сеть Bitcoin была проведена в июле 2015 г.

Цепочка блоков, как правило, является наименее уязвимым узлом используемой блокчейн-технологии, но в любом случае специалистам по информационной безопасности не следует забывать о существующих рисках, особенно для блокчейнов с новыми и недостаточно опробованными на практике методами достижения консенсуса.

Ошибки в ПО

Мощный удар по вере в принцип In Code we trust был нанесен в 2016 г. При атаке на The DAO (децентрализованную автономную организацию, созданную на платформе Ethereum) злоумышленник не нарушал правила, а использовал логическую ошибку в алгоритме, позволяющую повторно выводить уже потраченные средства. Деньги перечислялись из кошелька, но из-за временного разрыва сразу не снимались, так что появлялась возможность организовать «насос»: получающий кошелек возвращал уже потраченные средства и удваивал сумму в кошельке злоумышленника.

Часть денег участники смогли спасти, выведя их из децентрализованной организации на другие кошельки, но итог все равно впечатлил: украденная сумма превышала 50 млн в долларовом эквиваленте.

Дата	Суть атаки	Причина	Похищенная сумма*
29.06	Взломана южнокорейская биржа Bithumb	Успешная атака на компьютер сотрудника с хищением персональных данных клиентов	1 млн
17.08	Взломан сайт ICO израильского проекта CoinDash, указан ложный ETH-адрес	Подозревается руководство	7,5 млн
18.08	Взломан легкий многопользовательский криптокошелек для Ethereum Parity	Ошибка Zero Day в программе	32 млн
21.08	Взломан сайт ICO проекта Enigma Catalyst и указан ложный ETH-адрес	Не заменен скомпрометированный пароль	500 тыс.
20.11	Стартап Confido удалил информацию с сайта и аккаунты в соцсетях	Фейковые организаторы	374 тыс.

*В долларовом эквиваленте

Таблица 2. Наиболее известные успешные атаки 2017 г.

Создатель блокчейн-платформы Ethereum Виталик Бутерин поставил на голосование вопрос об откате транзакций злоумышленника. Подавляющее число майнеров его поддержали, хотя остались и принципиальные сторонники неизменяемости кода, которые продолжили поддерживать старую ветвь, получившую название Ethereum Classic.

В код можно верить, но нельзя забывать о возможных ошибках программистов. Причем в проектах на основе технологии блокчейн их особенно много. Бывший председатель совета Bitcoin Foundation Питер Вессенес оценил среднее количество ошибок в смарт-контрактах Ethereum как 100 на 1 тыс. строк кода, в среднем по криптовалютной отрасли – 15–50. Для сравнения: компания Microsoft выпускает код с 0,5 ошибок на 1 тыс. строк.

Традиционные угрозы

Для блокчейн-решений актуальны и традиционные риски информационной безопасности. В апреле 2016 г. на криптовалютной бирже ShapeShift через программу удаленного администрирования на компьютере разработчика были украдены персональные данные пользователей. В результате атаки удалось похитить сумму, эквивалентную $600 тыс. Халатность и мошенничество сотрудников, социальная инженерия, не

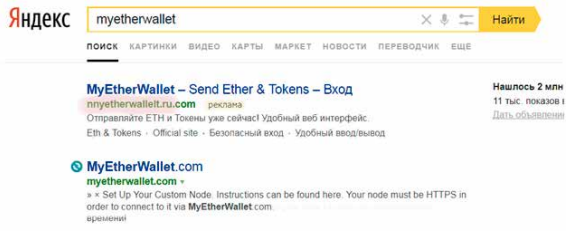


Рис. 2. Фишинговый сайт ловит невнимательных пользователей кошелька MyEtherWallet

измененные скомпрометированные пароли – вот причины наиболее крупных хищений в 2017 г. (табл. 2).

По-прежнему представляют проблему фишинговые сайты. Набрал в поисковике «Яндекс» название криптокошелька для Ethereum и получил в результатах поиска на первой позиции фишинговый сайт, где в доменном имени незаметно изменены буквы (рис. 2).

Резкий рост рынка ICO в 2017 г. не остался незамеченным для мошенников. Новый нерегулируемый рынок привлек большое количество желающих украсть часть собираемых средств. Согласно данным компании Group-IB, каждое ICO атакуют в среднем около 100 раз в течение месяца. Среди атак – фишинг, дефейс (deface – подмена сайта во время ICO), DDoS, а также целенаправленные атаки с целью компрометации секретных ключей и получения контроля над счетами.

Неопределенный статус криптовалют зачастую не дает жертвам возможности обратиться за помощью в правоохранительные органы. Наиболее дальновидные участники начинают выделять часть собранных на ICO средств на информационную безопасность.

Новый рынок

Появляется все больше проектов, использующих блокчейн-технологии. Идет процесс легализации криптовалют. Появление спроса на анализ разрабатываемых на базе технологий блокчейн систем уже заметили компании, специализирующиеся на ИБ, и стали предлагать свои услуги. В основном они касаются традиционных рисков информационной безопасности, актуальных и для новых решений.

Общие рекомендации: использовать наилучшие практики защиты, проводить аудит кода, инфраструктуры, искать уязвимости в логике выполнения программ. Хорошим решением будет проведение тестов на проникновение. Классические решения области ИБ, включающие технические и организационные меры, вполне применимы и для блокчейн-технологий.

О безопасности решения нужно думать уже на стадии разработки проекта – о запрете на изменение данных и приложений в сети, о предотвращении доступа к конфиденциальной информации со стороны любого пользователя, о защите ключей шифрования. И не стоит забывать о специфических вопросах, связанных с безопасностью консенсуса, особенно в проектах, использующих PoS.

Рынок блокчейн-технологий и криптовалют стремительно растет, есть проблемы информационной безопасности, есть платежеспособные клиенты и компании, которые могут им помочь. Есть все предпосылки для развития нового рынка услуг ИБ. ИКС

Безопасность 5G: угрозы из прошлого и надежды на будущее

Переход на сети пятого поколения не решает существующих проблем информационной безопасности и приводит к появлению новых угроз.

Николай Носов

Эксперты утверждают, что интернет вещей станет драйвером развития информационных технологий. Лавинообразный рост подключенных к интернету устройств требует новой инфраструктуры, увеличивающей число подключений к базовой станции мобильной сети. Ответом на новые запросы рынка стала разработка сетей связи пятого поколения, первая спецификация которых, 3GPP Release 15, утверждена в декабре 2017 г. Эта спецификация определяет радиоинтерфейс сети 5G, работающей на инфраструктуре сети LTE (4G).

Согласно утвержденной правительством госпрограмме «Цифровая экономика Российской Федерации», в 2020 г. сети 5G должны заработать в восьми городах России. С приходом сетей пятого поколения потребление трафика, по оценке аналитиков «Ростелекома», до 2025 г. увеличится в 20 раз.

К 2023 г., по прогнозу компании Ericsson, в сетях 5G будет зарегистрирован 1 млрд подключений (рис. 1). Услуги на базе 5G к этому времени станут доступны для 20% мирового населения. Будет собираться огромное количество данных.

Безопасность больших данных

Новые технологии несут новые риски. В январе 2018 г. в интернете появилась карта с передвижениями пользователей фитнес-трекеров (рис. 2), по которой журналисты проследили маршруты солдат на американских военных базах и секретных объектах. На ней можно рассмотреть, например, детальную карту американской базы в Кандагаре в Афганистане или месторасположение базы сил специальных операций США в сахельской саванне в Африке.

Анализ огромного количества данных, которые будут собираться в сетях 5G, даст возможность получить новые знания о предприятиях, странах и людях. Эти знания могут быть использованы для влияния на людей и страны, для силовых операций, шпионажа и вербовки.

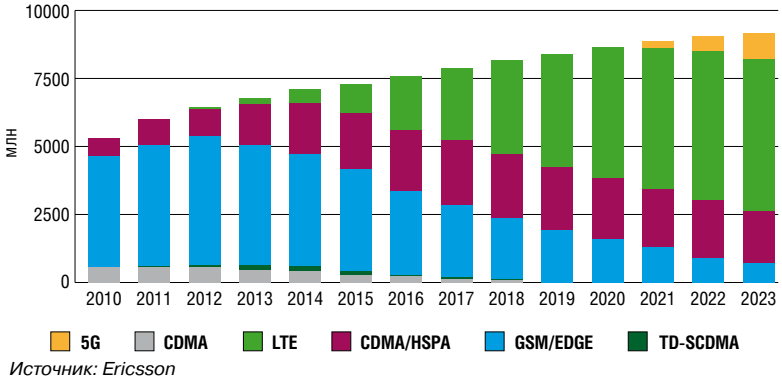
Многие государства осознали важность больших данных. России тоже надо думать об общих проблемах безопасности, возникающих, когда государство не может контролировать свои большие данные. Так, США, по словам гендиректора компании «Микрон» Гульнары Хасьяновой, уже задумались о создании национализированной (и построенной на оборудовании американских производителей) беспроводной сети 5G, которая должна помочь им защититься от иностранного влияния, в частности со стороны Китая. Предложенный Г. Хасьяновой рецепт не нов – локализация поставщиков оборудования для телекома и развитие своей элементной базы.

Проблемы управления и контроля

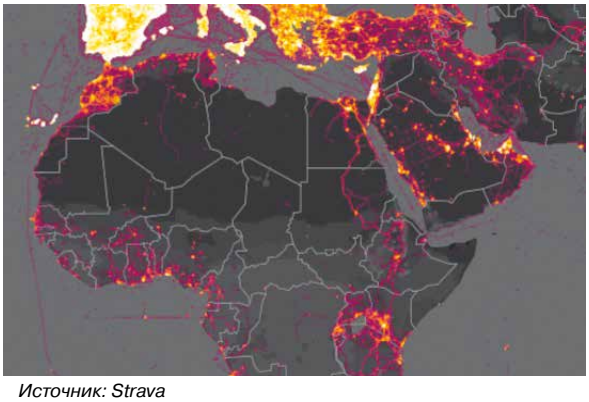
Осенью 2016 г. с помощью устройств интернета вещей была проведена атака на американскую компанию Dyn, которая привела к сбоям в работе большого числа сетевых сервисов глобального значения. Стали недоступны Twitter, Netflix, Airbnb, Reddit, газета The New York Times и многие другие. Ботнет Mirai, при помощи которого осуществлялась атака, заражал микропрошивки IoT-устройств, владельцы которых не поменяли стандартные пароли.

Сейчас к базовой станции может подключиться порядка тысячи абонентов. В сети 5G – уже до 65 тыс. Больше подключений, больше конечных устройств, больше уязвимостей. Ситуацию будет крайне сложно держать под контролем. И дело не только в стандартных паролях, нужно по-

Рис. 1. Рост числа подключенных устройств различных технологий в мировом масштабе



Источник: Ericsson



Источник: Strava

Рис. 2. Карта активности трекеров на Ближнем Востоке и в Африке, 2015–2017 гг.

стоянно следить за появляющимися уязвимостями и своевременно проводить обновление программного обеспечения и прошивок устройств.

Нужны умные сетевые устройства, прежде всего на границе сети (edge). Требуются умные сети, упрощающие автоматизацию развертывания того или иного участка сети, оценку и прогнозирование ее состояния, анализ данных о подключениях и перемещениях беспроводных устройств. Такие сети автоматизируют многие процессы обеспечения информационной безопасности: сегментацию на основе политик, контроль подключений пользователей и устройств, блокировку скомпрометированных подключений.

Сети 2G – источник угроз

Сети мобильной связи во всем мире связаны между собой, чтобы операторы могли предоставлять услуги роуминга путешествующим абонентам. При этом задействуются сети 2G и 3G, работающие с сигнальным протоколом SS7, который был разработан еще в 1975 г. Он фактически не имеет защиты и в настоящее время безнадежно устарел.

Используя SS7, можно обнаружить и отследить практически любого жителя планеты, просто зная его телефонный номер. Взломавшие протокол хакеры могут не только организовать прослушку и DDoS-атаки, но и перехватывать SMS-сообщения.

В прошлом году появилась информация о случаях обхода таким способом двухфакторной аутентификации банков. Как сообщала немецкая газета Süddeutsche Zeitung, злоумышленники с помощью вредоносного ПО и фишинга получали информацию о номере телефона и банковском аккаунте жертвы, а потом переводили с ее счета средства, перехватывая SMS-сообщение с кодом подтверждения и направляя его на свой телефонный номер.

Отказаться же от поддержки сетей 2G операторы связи не могут, так как они пользуются спросом, прежде всего по экономическим причинам. Не все хотят менять хорошо работающие датчики, поддерживающие 2G-связь, да и замена их на 4G-устройства, существенно более дорогие, обойдется в копеечку.

Если есть спрос, будет и предложение. Остается искать варианты снижения рисков использования сетей 2G. Руководитель отдела разработок компании «Аванпост» Александр Махновский подтвердил появившиеся у клиентов опасения по поводу безопасности двухфакторной идентификации в сетях 2G. По его мнению, альтернативой может служить использование технологии одноразовых паролей TOTP (Time-based One Time Password Algorithm), значительно снижающей вероятность успешной атаки.

Ждем нового релиза

Каждое новое поколение сетей снижало риски информационной безопасности. Не должны стать исключением и сети 5G, ведь их развертывание будет способствовать расширению списка объектов, привлекательных для организации кибератак. Киберпреступники могут использовать оборудование как точку входа к ресурсам предприятия или дома, есть риски клонирования параметров оборудования и «подмены» устройств, проведения DDoS-атак с использованием устройств интернета вещей. Для сетей 5G предполагается специфицировать целый ряд мер безопасности: обеспечение целостности и конфиденциальности системы сигнализации, аутентификацию и конфиденциальность абонентского оборудования, самих абонентов и их данных, защиту от кибератак, включая DDoS, атаки типа «человек посередине», атаки повторного воспроизведения и др. Ожидается, что эти меры будут определены в следующих релизах спецификаций 5G. Консорциум 3GPP предполагает выпустить вторую версию Release 15 к июлю 2018 г., а окончательную версию – к июлю 2019 г. А до тех пор...

Пока базовые станции сетей пятого поколения будут работать в режиме совместимости с сетью 4G. Однако, как показали исследования компании Positive Technologies, в инфраструктуре 4G могут быть реализованы те же атаки, что и в сетях на основе SS7. Критически опасные уязвимости протоколов DIAMETER и GTP, а также ошибки в конфигурации сетей – открытая дверь для злоумышленников, стремящихся похитить конфиденциальные данные абонентов, незаконно определить их местоположение, осуществить мошеннические действия или вызвать отказ в обслуживании клиентских сервисов. Руководитель группы исследований отдела экспертизы по безопасности телекоммуникационных систем Positive Technologies Павел Новиков сетует: «Остаются сети 2G, где на радиоэфире используется нестойкое шифрование, взламываемое за пару минут. Но на это сейчас мало кто обращает внимание. Голос до сих пор передается через 2G или 3G. При звонке по LTE мы все равно переключаемся на эти технологии. И никто не хочет вкладываться в исправление старых ошибок, которые давно существуют».

Сети 5G будут использовать новый протокол (по всей видимости, это будет не DIAMETER), но говорить об их безопасности рано. Учитывая, что новые интерфейсы не готовы, стоит ожидать, что первое время (которое может растянуться на десятилетие) сети 5G будут работать на ядре 4-го поколения со всеми его уязвимостями и недостатками. ИКС

Однофазные ИБП с двойным преобразованием

Компания Schneider Electric представила новую линейку ИБП среднего ценового сегмента APC Easy UPS Online серии SRV, предназначенных для обеспечения бесперебойного питания оборудования с высокой плотностью энергопотребления: серверов, сетей голосовой связи и передачи данных, медицинских лабораторий и небольших промышленных установок.

Модельный ряд покрывает мощностной диапазон от 1 до 10 кВА, устройства доступны как в стоечном, так и в напольном исполнениях. В настоящее время на рынок выпущены первые три модели SRV3KI, SRV6KI, SRV10KI мощностью 3, 6 и 10 кВА соответственно.

Время работы ИБП при полной нагрузке – от 2 до 4 мин, перезаряд до 90% емкости занимает 3–4 ч. Даже в проблемных сетях этого времени достаточно для обеспечения стабильной работы подключенного оборудования. ИБП серии SRV работают с входным напряжением широкого диапазона от 110 до 300 В и мало чувствительны к колебаниям в сети электропитания, что позволяет использовать их в условиях устаревшей энергосистемы, характерной для ряда российских регионов.

Применение температурной компенсации увеличивает срок службы используемого в ИБП аккумулятора, а специальная защита предотвращает возможное повреждение элементов ИБП при достижении слишком высокого напряжения. В режиме экономии энергии при качественном электропитании некоторые модули ИБП не задействуются, что значительно повышает эффективность его работы без ущерба для защиты устройств и систем.

Контроль за состоянием ИБП APC Easy UPS Online серии SRV можно осуществлять при помощи ЖК-дисплея. При изменении мощности электросети и режима работы устройства подается звуковой сигнал. Удаленный мониторинг и управление ИБП и подключенным оборудованием возможны через Ethernet-соединение.

Все устройства серии построены по технологии двойного преобразования (online). Это решение позволяет обеспечить идеальное выходное напряжение при практически любых неполадках в электросети и добиться отсутствия разрыва при переключении из рабочего режима в автономный и обратно, гарантируя отсутствие переходных процессов.

www.apc.com

Интеллектуальные PDU

Линейка Smart-PDU RPCM (Resilient Power Control Module) – продукты компании RCNTEC, которые объединяют в себе функции удаленного управления, автоматического ввода резерва (АВР) без прерывания работы подключенного оборудования, защиты от короткого замыкания на каждом выводе, счетчика электроэнергии с учетом активной и реактивной мощности, индикации корректно подключенного заземления, а также функцию настраиваемых порогов потребления тока на каждом выводе и возможность корректно задавать последовательность и задержки при включении устройств после полного обесточивания.

Модуль RPCM производится в трех моделях: 16A, 32A и 63A Mining Edition.

Устройства RPCM (16A, 32A) предназначены для использования как в корпоративном сегменте для модернизации и упрощения инфраструктуры ЦОДа, повышения надежности, отказоустойчивости систем и снижения совокупной стоимости владения, так и в частном сегменте, например в домовладениях – для защиты от пожаров и коротких замыканий.

RPCM Mining Edition – специализированное решение для владельцев майнингового оборудования, позволяющее повысить пожарную безопасность, защититься от коротких замыканий и автоматизировать перезапуски зависающего майнингового оборудования, позволяя технически защитить инвестиции и повысить эффективность майнинга.

Вся функциональность интеллектуальных PDU доступна для мониторинга и управления через полный набор интерфейсов управления. Это интуитивные и простые в использовании веб-интерфейс и интерфейс SSH Command Line.

С помощью протоколов REST API и SNMP Smart-PDU RPCM могут интегрироваться с любыми биллинговыми системами и системами мониторинга, позволяя клиентам включать/перезагружать/выключать любой физический сервер из биллинговой консоли.

В магазине AppStore доступно бесплатное мобильное приложение для дистанционного управления RPCM для iPhone и iPad.

Все модели Smart-PDU RPCM имеют сертификаты соответствия нормам электробезопасности, принятым Европарламентом, а также сертификаты пожарной безопасности.

RPCM разработаны и производятся в России.

www.rcntec.com

Мощный кинетический накопитель

Компания Piller представила PowerBridge PB60+ – модель кинетического накопителя, предназначенного для применения в системах ИБП без аккумуляторных батарей.

Устройство отличается компактностью и рассчитано на работу с нагрузкой свыше 3 МВт, что позволяет обеспечить время автономной работы нагрузки мощностью 1 МВт в течение 60 с и более. PB60+ имеет низкий уровень потерь и требует минимального обслуживания.

Технические характеристики кинетического модуля PB60+:

- мощность – 3600 кВт;
- запас энергии – 60 МДж;
- габариты (Ш × Г × В) – 1674×1674×2133 мм;
- рабочий диапазон температур окружающей среды – 0...+50°C;
- относительная влажность окружающей среды – не более 95% (без образования конденсата);
- высота над уровнем моря (без ухудшения характеристик) – 1000 м.

Установка ИБП Piller UBT+, состоящая из синхронного мотор-генератора Uniblock и накопителя PB60+, позволяет легко интегрировать в единую систему ИБП внешние дизель-генераторные или газогенераторные установки в качестве резервных источников мощности.

www.piller.com

ИБП для защиты домашней и офисной техники

ИБП «Импульс» серий «Юниор» и «Юниор смарт», разработанные ЦРИ «Импульс», предназначены для защиты электропитания домашней и офисной техники: ПК, рабочих станций, периферийного оборудования, кассовых аппаратов, торговых терминалов и пр.

Мощность устройств серии «Юниор» составляет 450–1000 ВА, серии «Юниор смарт» – 600–2200 ВА. Все модели семейства «Юниор» оснащены встроенным стабилизатором напряжения AVR, что позволяет поддерживать выходное напряжение в пределах нормы при пониженном или повышенном напряжении электросети.

Устройства серии «Юниор» и «Юниор смарт» относятся к категории линейно-интерактивных ИБП и выдают ступенчатую аппроксимацию синусоиды на выходе устройства. ИБП рассчитаны на работу от электросети с напряжением от 162 до 290 В переменного тока с частотой 50–60 Гц.

Серия «Юниор» – устройства с минимальным количеством органов управления и индикации для простой эксплуатации без лишнего функционала. Они помещены в компактный корпус и имеют выходные разъемы типа IEC 320 C13. Модели ИБП серии «Юниор» 450–850 ВА способны обеспечить защиту до четырех устройств с совокупной потребляемой мощностью согласно заявленным техническим характеристикам. В модели «Юниор» 1000 ВА также предусмотрены встроенные системы защиты от перегрузки и короткого замыкания на выходе.

Модели серии «Юниор смарт» 600–2200 ВА тоже помещены в компактный корпус, но обладают уже бóльшим функционалом. Устройства имеют ЖК-дисплей на передней панели, который отображает текущие параметры их работы. Встроенный USB-контроллер позволяет передавать эти параметры в компьютер с помощью USB-кабеля, входящего в комплект поставки. С помощью специального ПО можно отслеживать не только текущие параметры работы устройства, но и календарь его активности, а также проверять состояние ИБП. Модели «Юниор смарт» имеют на выходе розетки типа Schuko для подключения внешних устройств. Кроме того, на задней панели ИБП имеются разъемы USB, RS232 для подключения к компьютеру и RJ45 для защиты телефонных и модемных линий.

Модели серий «Юниор» и «Юниор смарт» являются устройствами plug & play и не требуют специальных знаний для установки, настройки и эксплуатации.

www.impuls.energy

Перечень публикаций журнала «ИКС» за 2017 г.

НОВОСТИ

ТЕМА НОМЕРА

Бизнес как сервис . . . . . № 1–2

Фокус
Бизнес как сервис. Сервис как бизнес
П. РАСТОПШИН. Что отдавать на аутсорсинг?
С. ЕРИН. Чем BaaS отличается от SaaS?
В. ГАЙЛИТ. Крупному бизнесу нужен инсорсинг
Проект
М. ЗИГАНШИН. Пицца как сервис
И. ПЯТИН. Облачная биржа автомобилей
Гуру
А. САЛОВ. Ларек в облаках
Ракурс
А. СОКОЛОВСКИЙ. Казахстан: дать шанс национальной ИТ-индустрии
В. МАКАРОВ. Сервисная модель не тренд, а целесообразность каждый раз
О. СИМАКОВ. Нужна конкуренция сервис-провайдеров
Д. БЕССОЛЬЦЕВ. Импортозамещение как аутсорсинг бизнес-функций
Особое мнение
Ю. САМОЙЛОВ. BaaS? Мы не оказываем такого рода услуги
Подробности
В. БОЧКАРЕВ. Чем проще сервис, тем сложней
В. ЕСКИН. Спасение как сервис
Ю. БРАЖНИКОВ. SECaaS как бизнес
М. ВОЛКОВ. Что нужно знать при переходе на сервисную модель
Концептуальный поворот
А. АРХИПОВ. Будущее в децентрализации
Дискуссионный клуб «ИКС»
Сервис – кому какой?
Бизнес-партнер
М. ФИННИ. Глобализация бизнеса и цифровая трансформация

О спорт, ты – IT! . . . . . № 3–4

Фокус
Спортивное ИТ-поведение
Позиция
А. ЧЕРНЕНКО. На стыке консерватизма и инноваций
Игроки
С. БУЛАНЧА. Не только умощнение бренда
Ракурс
Стадион для мундиала
А. НОВИКОВ. Спортивное строительство не место для экспериментов
А. БОНДАРЬ. Стадион разумный
А. БАШМАКОВ. Спортивные нагрузки оператора
А. ЧУВИЛИН, А. ВОРЮХИН. Крупный стадион – что большой ЦОД
С. ШЕСТАКОВ. Слаботочка для стадиона
Л. ВАРУКИНА. Стадион мобильный
О. ГОЛОСОВ. Могут ли ИТ помочь забить гол?
Дискуссионный клуб «ИКС»
Аналитика вместо допинга
Модель
Р. БОГАУТДИНОВ. «Картинка» Олимпиады – бесценна
Т. ВЕКИЛОВ. Не экономить на безопасности

Новый Телеком . . . . . № 5–6

Фокус
Телеком вырабатывает новое лицо
Модель
А. РОКОТЯН. Спорные мысли об аутсорсинге сетевой инфраструктуры
И. ЕГОРОВ. Совместное использование инфраструктуры для операторов все актуальнее
Ракурс
Д. ЛИ. Digital с человеческим лицом
Е. АЛЕКСЕЕНКО. В сторону формирования B2B-платформы

ДЕЛО

■ «ИКС» proТЕХнологии

Реклама в номере

Указатель фирм и организаций

Учредители журнала «ИнформКурьер-Связь»:

ООО «ИКС-Медиа»:
127254, Москва,
Огородный пр-д, д. 5, стр. 3;
тел.: (495) 785-1490, 229-4978.

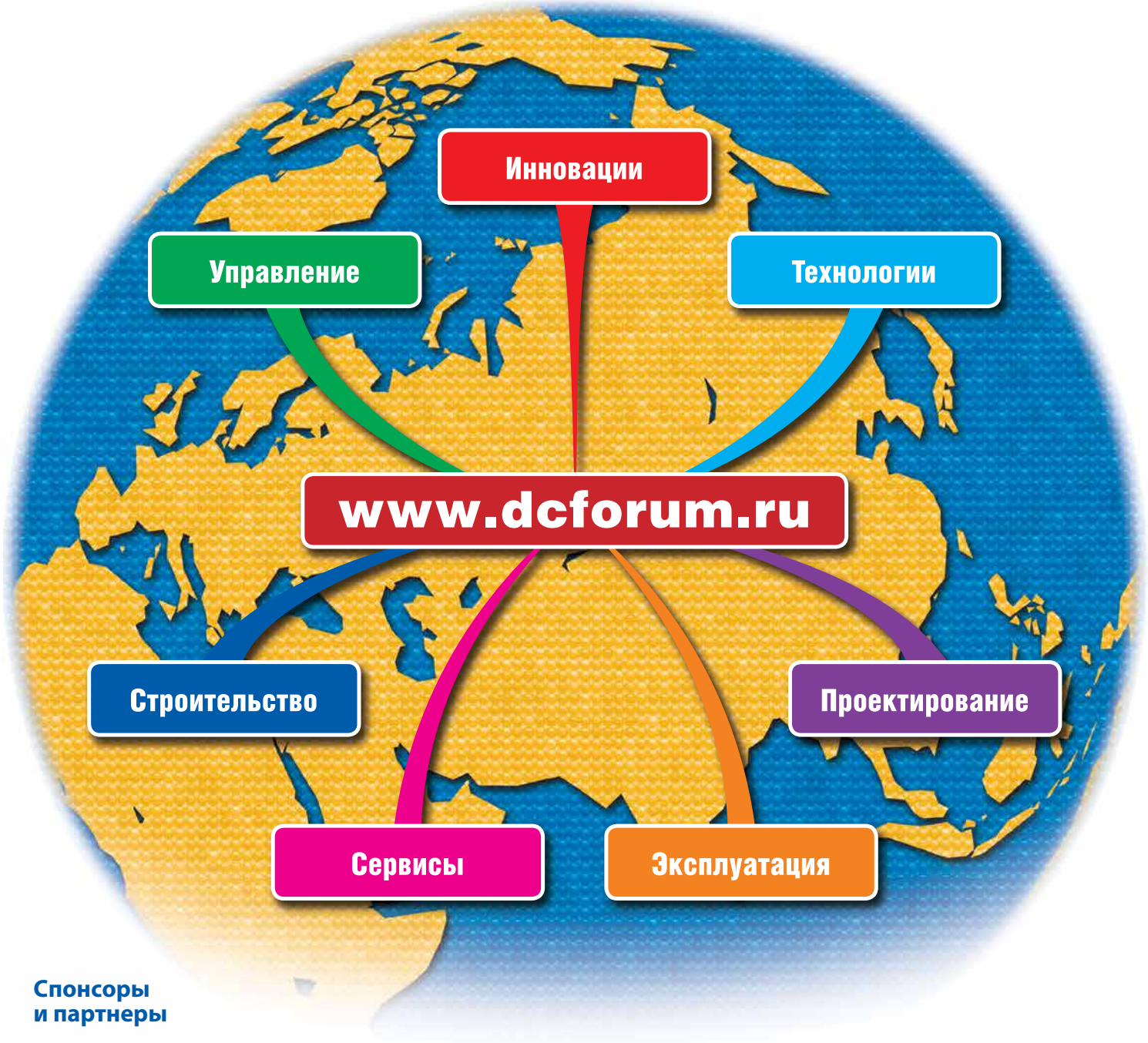
МНТОРЭС им. А.С. Попова:
107031, Москва, ул. Рождественка,
д. 6/9/20, стр. 1;
тел.: (495) 921-1616.

13-я международная конференция

ЦОД

13 сентября 2018
Москва, Центр Digital October

XIII DATA CENTER FORUM



Спонсоры и партнеры

Life Is On Schneider Electric
RITTAL
DKC
HTS HOSSER TELECOM SOLUTIONS
CABERO HEAT EXCHANGER
POWERCONCEPT ПРОМЫШЛЕННЫЕ АККУМУЛЯТОРЫ
СЭ SOLUTIONS КАЧЕСТВЕННО.СДЕЛАНО.В РОССИИ.
ИМПУЛЬС ИСТОЧНИКИ БЕСПЕРЕБОЙНОГО ПИТАНИЯ
ОРБИС СОЛЮШНС
ТИСКОМ

Доступный уровень защиты вашего бизнеса **с ИБП APC серии SRV**

Новые ИБП APC Easy UPS Online (1–10 кВА) с технологией двойного преобразования среднего ценового сегмента предназначены для обеспечения бесперебойного питания оборудования с высокой плотностью энерговыделения.

- Высокий коэффициент мощности
- Интеллектуальное управление батареями
- Режим экономии энергии
- Возможность параллельной работы делают эти ИБП незаменимыми в условиях нестабильной электросети

Модель **SRV3KI**

Модели **SRV6KI, SRV10KI**

Узнайте подробнее на www.apc.com

Наши специалисты помогут вам подобрать идеальное решение для ваших бизнес задач, свяжитесь с нами по телефону **8-800-200-64-46** (звонок по России бесплатный)

Life Is On

APC™ by Schneider Electric