

разных задач. Например, для идентификации без используемой в настоящее время сложной системы выпуска ключей. Можно перевернуть систему с ног на голову. Люди могли бы сами выпускать свои ключи, а затем удостоверяют их, например, в банках или прямо записывать в ЕСИА. В этом случае у людей на руках достаточно быстро оказалось бы большое количество работоспособных ключей, которыми они могли бы оперативно пользоваться для получения удаленных услуг. А технология блокчейн очень подходит для хранения таких ключей.

Другая возможная область применения технологий распределенного реестра – передача государством своих бизнес-процессов, связанных с регистрацией прав (собственности и т.д.), на аутсорсинг в децентрализованную систему, сертифицированный блокчейн.

Финансы и банки

Еще одна область применения технологий распределенного реестра – финансы. Можно отказаться от банков как системы для перевода денег. Немного парадоксально – но наличные деньги можно рассматривать как своего рода блокчейн без банков. Их выпускает Центральный банк. Люди без всяких коммерческих банков этими наличными деньгами обмениваются и прекрасно себя чувствуют. Идея о том, что вместо наличных физических будут выпускаться электронные

деньги, мне кажется тривиальной. Все говорят о том, что надо переходить от бумажного документооборота к электронному. А чем тогда деньги отличаются от бумажных документов? Если надо переводить всё в электронную форму, то и деньги тоже. Действительно, вместо наличных денег центральные банки могли бы выпускать наличные электронные деньги. И не использовать коммерческие банки для их распространения или расчетов. Или задействовать банки только для первичной выдачи людям электронных наличных. Но, честно говоря, я не думаю, что в ближайшие пять лет в какой-либо крупной стране это произойдет.

Услуга «банк как сервис» быстро не уйдет в блокчейн. Все-таки финансовая сфера очень инерционна. Люди, занимающиеся финтехом и инновациями, энергичны и готовы ко всему новому. Но массовый потребитель консервативен и будет долго присматриваться, принюхиваться, пробовать новые продукты. Минимум пять лет уходит на то, чтобы какой-либо новый продукт начал играть существенную роль в жизни людей.

Будет плавный процесс. Биткойн запустили в 2009 г., но только в начале 2016-го – через шесть лет – об этом явлении стали говорить всерьез. Несмотря на то что сейчас изменения в нашей жизни происходят гораздо быстрее, широкое внедрение технологий распределенного реестра займет пять-семь лет. ИКС

Сервис: кому – какой?

Что нужно клиенту от провайдера сервисных услуг? Какие сервисы пользуются наибольшей популярностью? Чего опасается заказчик и насколько его страхи обоснованы? Поинтересуемся мнением участников рынка.



«ИКС»: Какие ИТ-сервисы вам чаще всего отдают на аутсорсинг?

Андрей МЕЛУЗОВ, директор по развитию департамента ИТ-аутсорсинга, ГК «КОРУС Консалтинг»: В основном мы наблюдаем спрос на передачу функций поддержки сложных инфраструктурных решений. Для их сопровождения требуется глубокая экспертиза со стороны ИТ-команды, а ее отсутствие заметно влияет на бизнес-процессы. Клиентам же удерживать сильных инженеров сложно – для них не всегда есть интересные задачи и часто уже достигнуты потолки зарплат.

Большим спросом пользуется и сопровождение удаленных площадок. Инцидентов на

них возникает немного, но каждый необходимо устранить в кратчайшие сроки. И здесь также есть сложности с квалифицированными инженерами, которым неинтересно месяцами ждать возможности проявить свое мастерство.

Оба типа услуг популярны в ритейле, банковской индустрии и телекоме – везде, где есть распределенные площадки и где бизнес сильно зависит от ИТ.

Помимо этого, заказчики стали чаще обращаться с запросами на сопровождение инженерных систем, например, кондиционирования. Все более востребованной становится модель работы, при ко-



А. МЕЛУЗОВ

торой нам на сопровождение передают ряд контрактов текущих поставщиков. Это актуальная услуга для компаний, работающих более чем с десятком подрядчиков.

Денис ШИРОКИЙ, заместитель гендиректора, МТТ: Сейчас становятся популярными инструменты для повышения конверсии и продаж. В частности, услуга call back, которая позволяет вдвое увеличить прием заявок с сайта. С нашей точки зрения, перспективны решения по аналитике данных (включая онлайн-аналитику), которые интегрируются с социальными сетями и сервисами анализа голосового трафика. Мы также создаем на перспективу новые ценности, которые будут драйверами развития бизнеса наших клиентов. Например, сервисы аналитики голосового трафика, которые интересны как малому бизнесу, так и крупным игрокам, использующим услуги call-центров.

Андрей ЗАХАРОВ, руководитель департамента облачных сервисов, Linx-datacenter: Чаще всего нам на аутсорсинг отдают физическое размещение ИТ-оборудования в дата-центре. Это позволяет заказчику сэкономить на строительстве собственного ЦОДа и найме технических специалистов и сосредоточить ресурсы на развитии собственного бизнеса. Кроме того,



А. ЗАХАРОВ

растет спрос на размещение офисных приложений и хранение данных на облачных серверах.

Михаил ХОЛОПОВ, гендиректор, ATLEX.Ru: Сегодня клиент больше всего заинтересован в виртуализации инфраструктуры, резервном копировании информации, стриминге аудио и видео, работе со сложными базами данных и анализе «больших данных». С течением времени сервис-провайдерам чаще будут доверять второстепенные сервисы, которые нужны, но не критичны для работы компании. В руки хостеров полностью перейдут и сложные ИТ-процессы, для реализации которых непрофильной компании придется содержать штат администраторов.

Александр ДУБСКИЙ, руководитель направления «Непрерывность ИТ-сервисов и защита данных», КРОК: У нас высока доля проектов по аренде вычислительной инфраструктуры (IaaS). Растет спрос на резервное копирование как сервис, обеспечение катастрофоустойчивости и непрерывности бизнеса, построение гибридных инфраструктур и другие сервисы, предоставляемые на базе сети дата-центров. Со стороны зарубежных компаний повысился спрос на услуги миграции в российский ЦОД для соответствия закону о персональных данных.



А. ДУБСКИЙ



«ИКС»: Помогает ли бизнесу наличие сертификатов? Или заказчика больше интересует цена, предлагаемый функционал, рекомендации других клиентов?

Дмитрий САВЕЛЬЕВ, директор по развитию бизнеса сервисного центра, «Инфосистемы Джет»: Однозначно помогает. Для крупных заказчиков, госорганизаций, компаний с иностранным участием наличие сертификатов – одно из ключевых требований. Сертификат от вендора – это, как правило, гарантия высокого уровня поддержки, а также возможность получения дополнительных скидок или других преимуществ. А вот для организаций SMB-сегмента наличие у подрядчика вендорских статусов зачастую не столь принципиально.

А. ЗАХАРОВ: Да, помогают. На то, как заказчики выбирают партнера в сфере хранения и обработки критически важной информации, влияет совокупность факторов. Сертификаты – один из важных элементов оценочной матрицы, по сути, свидетельство об аттестации технических платформ и внутренних процессов провайдера от известной и авторитетной на ИТ-рынке компании, например Cisco Systems, Uptime Institute или Schneider Electric. Подобные системы сертификации воспринимаются как отраслевые стандарты. При прочих равных условиях клиент скорее выберет ЦОД, качество услуг которого подтверждено на таком уровне. Финансовая сфера, например, трепетно относится к наличию у ЦОДа сертифика-

тов безопасности PCI DSS. Есть клиенты, которые необходимость определенной сертификации дата-центров прописывают в условиях проведения тендеров. В то же время если заказчик ограничен в ресурсах, то, скорее всего, он будет выбирать ЦОД исходя из предлагаемых ему цен, а сертификация будет иметь меньшее значение.

М. ХОЛОПОВ: Как правило, сертификаты клиентов не интересуют. Предпочтение отдается компаниям с опытом успешных реализованных проектов, которые могут предложить функциональные решения за приемлемую цену. Можно сказать, что лучший сертификат – это рекомендации уже существующих клиентов.

Александр ФАЙНБОЙМ, руководитель направления ИТ-аутсорсинга, КРОК: Я бы сказал, что это отлично работало лет пять назад. Но сегодня всем приходится считать деньги, экономить и оптимизировать. Теперь заказчики в первую очередь обращают внимание на цены, и лишь потом разбираются, что в рамках указанной стоимости им предлагают. Тако-



А. ФАЙНБОЙМ

вы реалии современного российского рынка. В результате заказчик, погнавшись за дешевизной, часто приобретает услугу у не совсем компетентной компании. Естественно, что уровень квалификации та-

кого подрядчика напрямую отражается на удовлетворенности заказчика. А это, в свою очередь, приводит к тому, что компания разочаровывается в услуге в целом.



«ИКС»: Как вы оцениваете уровень защиты персональных данных и конфиденциальных данных у провайдера по сравнению с моделью размещения их у клиента?

Д. ШИРОКИЙ: Поскольку провайдер использует только сертифицированные и промышленные инструменты обеспечения безопасности и контроля утечек информации, размещение данных на его стороне сравнимо или даже более безопасно, чем хранение информации на стороне клиента. В зависимости от типа сервисов клиент всегда может получить на стороне провайдера дополнительное резервирование, необходимую пропускную способность или емкость каналов. Это обеспечит ему требуемую непрерывность бизнеса.



Д. ШИРОКИЙ

М. ХОЛОПОВ: Уровень безопасности, который может предложить хостинг-провайдер, несравнимо выше того, который клиент сможет организовать самостоятельно. Во втором случае высоки риски безопасности: в серверной комнате, построенной в условном офисе, нельзя обеспечить бесперебойность работы «железа» и зарезервировать вычислительные мощности. При аварийной ситуации специалист дата-центра в силу своих компетенций, опыта работы с оборудованием от разных производителей и знания различных типовых сценариев решения критических ситуаций никогда не совершит тех ошибок, которые может допустить сотрудник компании, не специализирующейся на хранении и обработке данных.

Если же говорить о физическом доступе к вычислительным мощностям, то, очевидно, что клиент не в состоянии предотвратить неправомерное проникновение к серверам, стоящим у него в офисе. А дата-центр – это объект охраняемый, и любое взаимодействие с «железом» строго регламентировано.

Но это не отменяет ряда сложностей, которые могут возникнуть у клиента, разместившего свои серверы в коммерческом ЦОДе. Российская действительность специфична: полномочия по изъятию оборудования есть у многих правоохранительных органов – полиции, прокуратуры, судебных исполнителей, ФСБ. Значит, в любой момент в дата-центр могут прийти «люди в форме» и конфисковать оборудование без суда и следствия. В Европе в этом смысле законодательство сдержаннее: получить доступ к серверам (и уж тем более изъять элементы ИТ-инфраструктуры) можно исключительно по решению суда. Это, конечно, совсем другой уровень обеспечения безопасности.

А. ФАЙНБОЙМ: Если заказчик не уделяет должного внимания вопросам инфобезопасности, то размещение данных в ЦОДе с надлежащим уровнем защиты будет для него настоящим спасением. Но бывают и обратные ситуации, когда компания с отлично выстроенной системой защиты начинает работу с сомнительным подрядчиком, который не в состоянии обеспечить адекватную защиту данных. Все очень ситуативно, и заботиться о защите должны обе стороны.



«ИКС»: Что посоветуете делать для обеспечения непрерывности работы бизнес-критических систем, находящихся на аутсорсинге?



М. ХОЛОПОВ

М. ХОЛОПОВ: Три золотых правила. Первое: если проект отдан на аутсорсинг, необходимо иметь менеджера проекта, который видит всю «картину мира» и координирует действия других сотрудников. Второе: продукт должен быть документирован, т.е. нужно иметь техническое задание как на продукт в целом, так и на каждую его часть. И третье: в вашем распоряжении, локально, должны быть актуальные исходные коды. Задача состоит в том, чтобы минимизировать зависимость проекта от одного человека или группы лиц.

А. ФАЙНБОЙМ: Важно правильно контролировать поставщика услуг. Не выполнять работу за него, а именно контролировать выполнение оговоренных ранее

KPI. Все должно быть регламентировано. Кроме того, можно не отдавать весь аутсорсинг в одни руки, иметь primary- и secondary-поставщика. Они могут работать на разных участках или параллельно, но суть в том, что при возникновении форс-мажора второй поставщик всегда может подстраховать первого.

А. ДУБСКИЙ: Следует начать с анализа и оценки рисков и разработки комплексной программы кризис-менеджмента (ВСМ) для всех ИТ-зависимых бизнес-процессов. Такие программы состоят из двух обязательных компонентов – плана по поддержанию бесперебойности бизнес-процессов и плана их восстановления в случае нештатных ситуаций. В стратегическом смысле программа ВСМ обеспечивает непрерывность бизнеса – устойчивость организации к всевозможным сбоям и инцидентам, простоям систем, разрушениям и потерям, в первую очередь – фи-

нансовым. Наличие проработанной BSM-программы жизненно необходимо кредитно-финансовой отрасли, крупным телеком-компаниям, высокотехнологичным предприятиям непрерывного производственного цикла – например, атомным электростанциям. На ряде рынков существуют специальные регламенты в отношении непрерывности бизнеса, которые должны соблюдаться для лицензирования деятельности.

А. МЕЛУЗОВ: Одним из самых действенных способов помогать подрядчику предоставлять лучший сервис могла бы стать привязка стоимости сервисов или штрафов к конкретным бизнес-показателям, например, к получению или неполучению части прибыли, которую обеспечивает поддерживаемый интегратором процесс или система. Но если на возмещение упущенной выгоды согласны многие заказчики, то к разделению доходов, к сожалению, готовы единицы. Мы также можем посоветовать скрупулезно составлять договор об уровне сервиса и учитывать в нем максимальное количество факторов, влияющих на качество проекта. Внимательно стоит изучить и степень зрелости

ИТ-процессов у интегратора – чем сильнее регламентирован проект, тем меньше риск, что сработает человеческий фактор.



Д. САВЕЛЬЕВ

Д. САВЕЛЬЕВ: Универсального рецепта, как обычно, не существует. Основные принципы – это тщательное планирование, включая оценку критичности систем, требований к SLA, отказоустойчивости и резервированию. Существует множество решений по обеспечению отказоустойчивости и быстрого восстановления. Важно совместно с провайдером выбрать наиболее подходящий способ. Кроме того, отдав что-либо на аутсорсинг, нужно продолжать измерять условную «температуру» систем (ключевые показатели эффективности), а также периодически проводить ревизию и вносить изменения, если необходимо. Ну и, конечно, один из ключевых факторов успеха – правильный выбор провайдера.



«ИКС»: Есть ли у вас примеры проектов, использующих модель «бизнес как сервис»?

М. ХОЛОПОВ: Ярким примером таких проектов можно считать интернет-магазины. Многие из них занимаются продажей товаров разных брендов под своим логотипом, т.е. клиент получает вещи от имени интернет-магазина, но склады, где эта продукция хранится, и вся логистика выстроены по схеме аренды бизнеса.

Д. ШИРОКИЙ: Да, например, мы предоставляем унифицированные коммуникации для корпоративных клиентов (ВАТС).

А. ЗАХАРОВ: Да, у нас есть пул партнеров среди операторов связи, которые не располагают собственными ЦОДами, но тем не менее имеют право предоставлять любые услуги наших дата-центров своим клиентам на основании партнерского контракта. Иными словами, мы даем операторам-партнерам возможность зарабатывать как на предложении наших услуг, так и на формировании собственных сервисов с добавленной ценностью на базе ресурсов и мощностей Linxdatacenter.



«ИКС»: Какие новые технологии будут в ближайшее время оказывать существенное влияние на рынок аутсорсинга ИТ?

Георгий МЕГРЕЛИШВИЛИ, директор департамента развития сервиса и аутсорсинга, «Сервионика» (ГК «Ай-Тек»): Вполне вероятно, что развитие когнитивных технологий, одного из направлений искусственного интеллекта, изменит облик контакт-центров и спектр предоставляемых ими услуг. В нем более значимую роль будут играть IVR-сервисы, мессенджеры, чаты. Этот формат выгоден для контакт-центров:



Г. МЕГРЕЛИШВИЛИ

в чате оператор может одновременно общаться с тремя-четырьмя пользователями, а в случае голосового общения – только с одним. Такой подход отражает существующую в обществе тенденцию перехода от телефонных звонков к текстовым сообщениям. Будущее за искусственным интеллектом, который уже сейчас может принимать

на себя стартовый уровень коммуникации: выяснение того, какая проблема возникла, и предложение типового решения.

Д. ШИРОКИЙ: В ближайшее время вследствие увеличения стоимости оборудования и реализации интеграторских решений будет более востребована услуга IaaS. Также будут набирать популярность по сравнению с привычным ПО в «коробках» сервисы SaaS. Сегодня быстро растут в относительных показателях сервисы Big Data и IoT, и в перспективе они сформируют значительные по объему рынки.



ПОЛНЫЙ ТЕКСТ Дискуссионного клуба читайте на

www.iksmia.ru