

НАША ЦЕЛЬ – клаудизм!?

Часть 1. Дорога в облака

Б.Гольдштейн, д.т.н., зав. кафедрой СПбГУТ,
А.Голышко, к.т.н., системный аналитик ГК "Техносерв" / rase07@inbox.ru

DOI: 10.22184/2070-8963.2018.72.3.46.52

Инфокоммуникационный мир давно идет мультисервисным путем через завалы "железа" и проприетарное ПО к вездесущим знаниям, вездесущей подключенности и вездесущим взаимоотношениям через облако. По экспертным оценкам, за последний год рост облачных предложений достиг 25%, в то время как рынок классической ИТ-инфраструктуры вырос лишь на несколько процентов. "Клаудизм" постепенно заменяет собой все то, что мы когда-то подразумевали под словом "связь".

Облака плывут, облака,
Не спеша плывут, как в кино.
А.Галич

"Модель Бога"

Не секрет, что человечество старается все существующее в природе воспроизвести с помощью технологий, чтобы потом как-нибудь приспособить для своих нужд. Поэтому мы уже летаем и плаваем, забираемся в тайны макро- и микромира, пользуемся средствами глобальной коммуникации, умеем резать, сшивать и даже кое-что лечить. Сверхновых, правда, пока не зажигаем, зато с имеющимся ядерным арсеналом что-нибудь зажечь сможем так, что впору вспомнить о Боге. Или по нашей технической традиции как-нибудь его представить. И тут же возникает интересный вопрос, пришедший на ум нашему коллеге, известному отраслевому эксперту Алексею Шалагинову, – почему многие мировые религии представляют Бога в виде облака или в виде человека на облаке?

Сегодня все мы уже готовы к тому, что ответом будет ИТ-модель Бога (где Богу доступно создание всего сущего в мире ИТ) в виде cloud computing, или облачных технологий. Соответственно, телекоммуникационная компонента, без которой невозможен доступ к Богу, может выполнять для "ИТ-ясновидящих" функции третьего глаза.

Собственно, инфокоммуникационный мир давно шел мультисервисным путем через завалы "железа" и проприетарное ПО

к вездесущим знаниям, вездесущей подключенности (connectivity) и вездесущим взаимоотношениям через облако. В современных инфокоммуникациях облачные вычисления являются эффективной сетевой архитектурой предоставления многопользовательского сетевого доступа в режиме "по требованию" к пулу коллективных вычислительных ресурсов – приложений, сервисов, хранилищ данных, серверов, которые абоненты в реальном времени задействуют для получения услуг и/или решения собственных задач и высвобождают после их завершения.

В рамках этой архитектуры пользователи по мере необходимости в автоматическом режиме задействуют облачные физические и виртуальные ресурсы, сетевые хранилища данных, серверное время, виртуальные машины и пр. с использованием различных стандартных механизмов доступа. Провайдеры, в свою очередь, объединяют в пул, динамически перераспределяют, резервируют, масштабируют свои вычислительные ресурсы для обслуживания большого числа потребителей, контролируют их использование, формируют отчеты об объеме оказанных услуг.

В облаках существуют три базовых модели обслуживания (рис.1):

- Cloud Software as a Service (SaaS) – облачное программное обеспечение (ПО) как услуга (рис.1a);

- Cloud Platform as a Service (PaaS) – облачная платформа как услуга (рис.1б);
- Cloud Infrastructure as a Service (IaaS) – облачная инфраструктура как услуга (рис.1в).

Модель SaaS облачного программного обеспечения как услуги предоставляет пользователям готовое прикладное ПО, разработанное, управляемое и обслуживаемое провайдером. Пользователь не берет на себя забот по установке, обновлениям и поддержке работоспособности оборудования и работающего на нем программного обеспечения, а лишь удаленно пользуется им, как правило, через веб-интерфейс или с помощью тонкого клиента. Пример самой массовой и часто используемой SaaS-услуги – сервис электронной почты типа Gmail или "Яндекс". Более специализированные SaaS-сервисы – онлайн-овые органайзеры, системы документооборота, совместного управления проектами и т.п. В малом и среднем бизнесе в режиме SaaS могут применяться системы CRM, биллинга и ERP.

В рамках модели PaaS – платформа как услуга – пользователю предоставляется доступ к использованию информационно-технологической платформы облачного провайдера, включающей операционные системы, системы управления базами данных, средства разработки, коммуникационное ПО. В этой модели вся информационно-технологическая инфраструктура, включая вычислительные сети, серверы, системы хранения, целиком управляется провайдером. Провайдером же определяется набор доступных для пользователей видов платформ и набор управляемых параметров платформ, а пользователю предоставляется возможность использовать платформы, создавать их виртуальные экземпляры, устанавливать, разрабатывать, тестировать, эксплуатировать на них прикладное ПО, динамически изменяя при этом количество потребляемых вычислительных ресурсов.

Модель PaaS предоставляет пользователям среду для разработки или настройки облачных приложений. Облачные функции масштабирования, управления доступом, организации многопользовательского режима уже включены в платформу и не требуют разработки силами пользователя. Провайдеры PaaS могут предлагать и разные другие службы, которые повышают эффективность работы сервиса (каталоги, средства безопасности и планирования, поддержку географически распределенных команд, рабочие процессы). Прекрасный пример PaaS – созданная компанией Amazon служба AWS Elastic

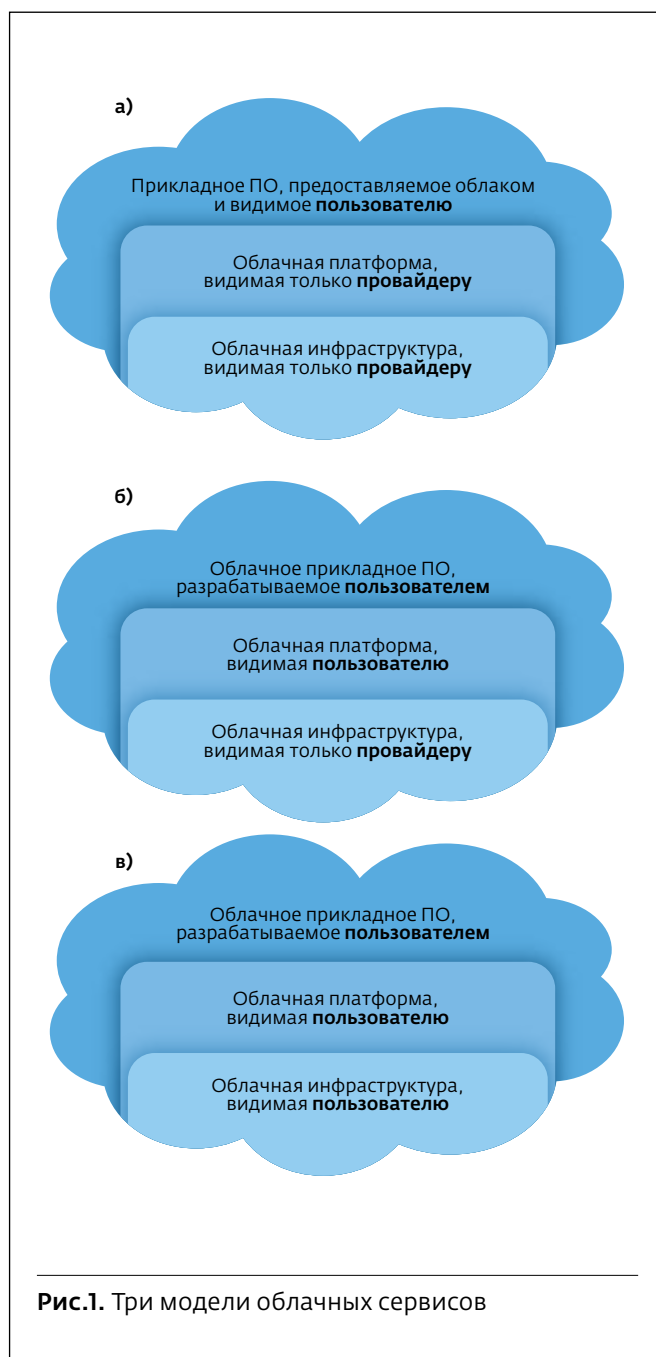


Рис.1. Три модели облачных сервисов

Beanstalk для развертывания и масштабирования веб-приложений и сервисов, разработанных на Java, .NET, PHP, Python, Ruby и др. Для написанного на этих языках и загруженного в систему кода Elastic Beanstalk автоматически выполнит развертывание: выделит ресурсы, организует балансировку нагрузки, автоматическое масштабирование и мониторинг работоспособности приложения. Пользователь при этом сохраняет полный контроль над ресурсами AWS и в любое время может получить к ним доступ.

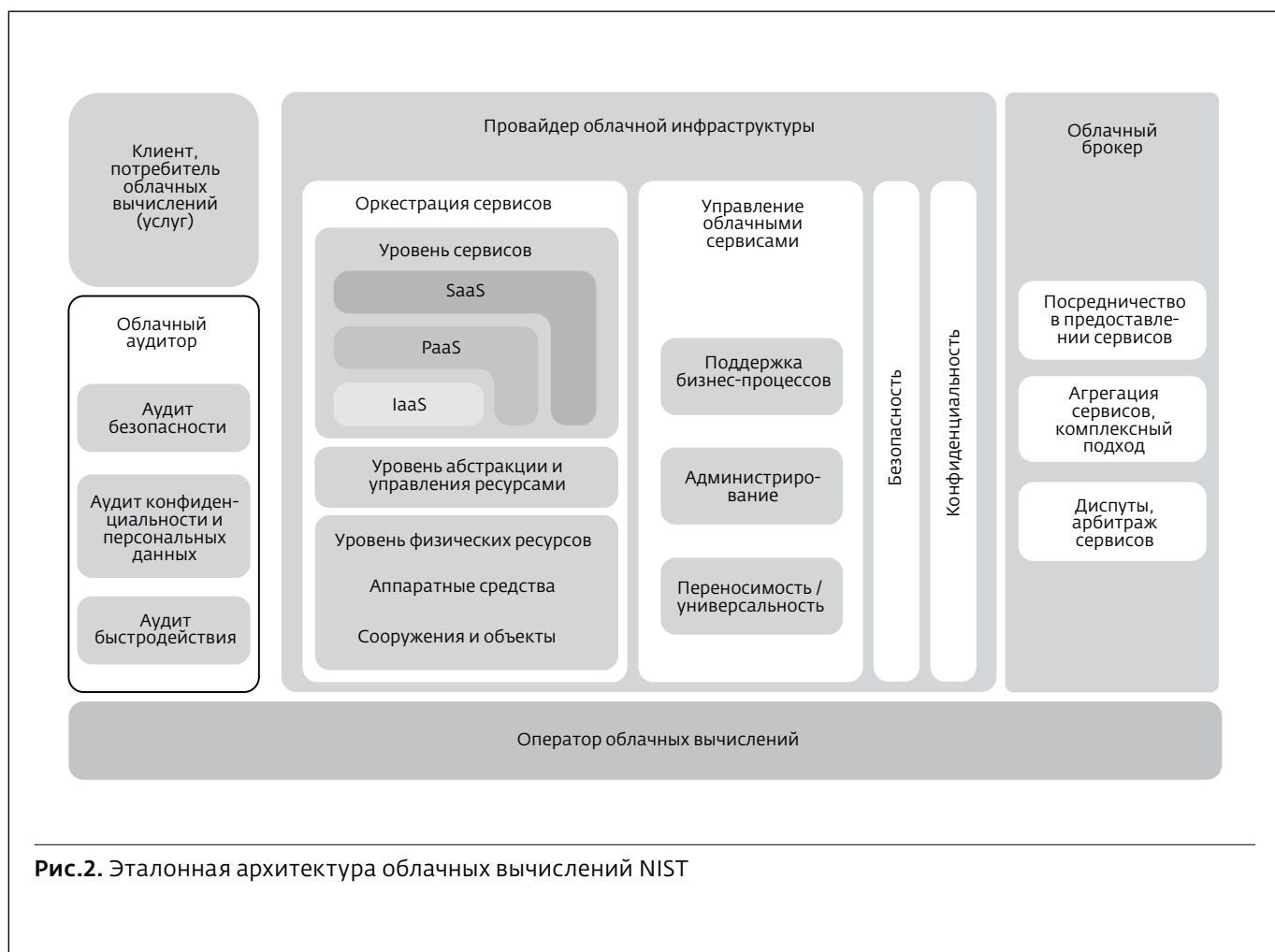


Рис.2. Эталонная архитектура облачных вычислений NIST

Модель инфраструктуры как услуги (IaaS) предполагает возможность задействования пользователем облачной инфраструктуры для самостоятельного управления вычислительными ресурсами, средствами обработки и хранения данных, сетями и другими фундаментальными вычислительными ресурсами, операционными системами, платформенным и прикладным ПО, некоторыми сетевыми сервисами. Управление же основной физической и виртуальной инфраструктурой облака, в том числе сети, серверов, типов используемых операционных систем, систем хранения данных осуществляется облачным провайдером. Мировыми лидерами IaaS являются компании Amazon, Microsoft, Google и IBM, но и в России компании большой тройки становятся провайдерами облачных платформ для крупного бизнеса. Например, МТС запустила IaaS-сервис облачных вычислений и облачного хранения данных #CloudMTS для крупного бизнеса на основе решения VMware, собственных ЦОДов и магистральной телекоммуникационной сети.

В Рекомендации ITU-T Y. 3500 Cloud Computing – Overview and Vocabulary в дополнение к SaaS, PaaS и IaaS предусмотрен ряд других облачных сервисов. Это Communications as a Service (CaaS) – сервисы, к которым относятся видеоконференции, веб-конференции, обмен мгновенными сообщениями и VoIP; Compute as a Service (ComaaS) – упрощенный вариант IaaS, охватывающий преимущественно облачный вычислительный ресурс; Data Storage as a Service (DSaaS), в рамках которого пользователь арендует пространство для хранения, резервного копирования данных и их передачи через интернет; Network as a Service (NaaS) – сервис, который включает виртуальную частную сеть VPN, настраиваемую маршрутизацию, протоколы многоадресной рассылки, брандмауэр безопасности, обнаружение и предотвращение вторжений, мониторинг и антивирус; Database as a Service, Desktop as a Service и др. Последние разработки в области облачных сервисов объединяются под названием XaaS, где X подразумевает произвольный набор

облачных сервисов в расширение базовой тройки SaaS, PaaS, IaaS (тот же смысл вкладывается и в термины Anything as a Service и Everything as a Service). Вполне прогнозируем интерес к совсем новым специализированным сервисам типа SecaaS (безопасность как услуга), IDaaS (идентификация как услуга), DRaaS (послеаварийное восстановление как услуга), BaaS (резервное копирование как услуга), Big Data-as-a-Service и др.

Эталонная облачная архитектура NIST

На рис.2 представлена эталонная архитектура облачных вычислений, разработанная NIST (National Institute of Standards and Technology). Она содержит пять главных действующих субъектов – акторов, каждый из которых выступает в своей роли, выполняет действия и функции. Эталонная архитектура NIST определяет пять представленных ниже акторов.

Пользователи облачных сервисов – люди или организации, обращающиеся за услугами к облачному провайдеру. Пользователями SaaS могут быть как организации, предоставляющие своим членам доступ к программным приложениям, так и конечные потребители, непосредственно использующие программные приложения,

а также администраторы приложений, настраивающие приложения для конечных потребителей. Пользователи PaaS могут применять инструменты и ресурсы, предоставляемые облачным провайдером, для разработки, тестирования и развертывания приложений, размещенных в облачной среде, а также для управления ими. В свою очередь, пользователи облачных вычислений IaaS задействуют облачные вычислительные ресурсы как виртуальные машины и хранилища данных.

Провайдеры облачных сервисов – люди или организации, предоставляющие облачные сервисы. Облачный провайдер может предоставлять один или несколько облачных сервисов, включая средства хранения и обработки данных, пользователям облачных вычислений в рамках каждой из трех моделей обслуживания (SaaS, PaaS и IaaS). Для SaaS провайдер также развертывает, настраивает, поддерживает и обновляет работу программных приложений в облачной инфраструктуре, чтобы сервисы предоставлялись облачным пользователям с ожидаемыми уровнями обслуживания. Для PaaS провайдер управляет вычислительной инфраструктурой платформы и запускает облачное ПО, которое предоставляет компоненты платформы, такие как исполняемый стек

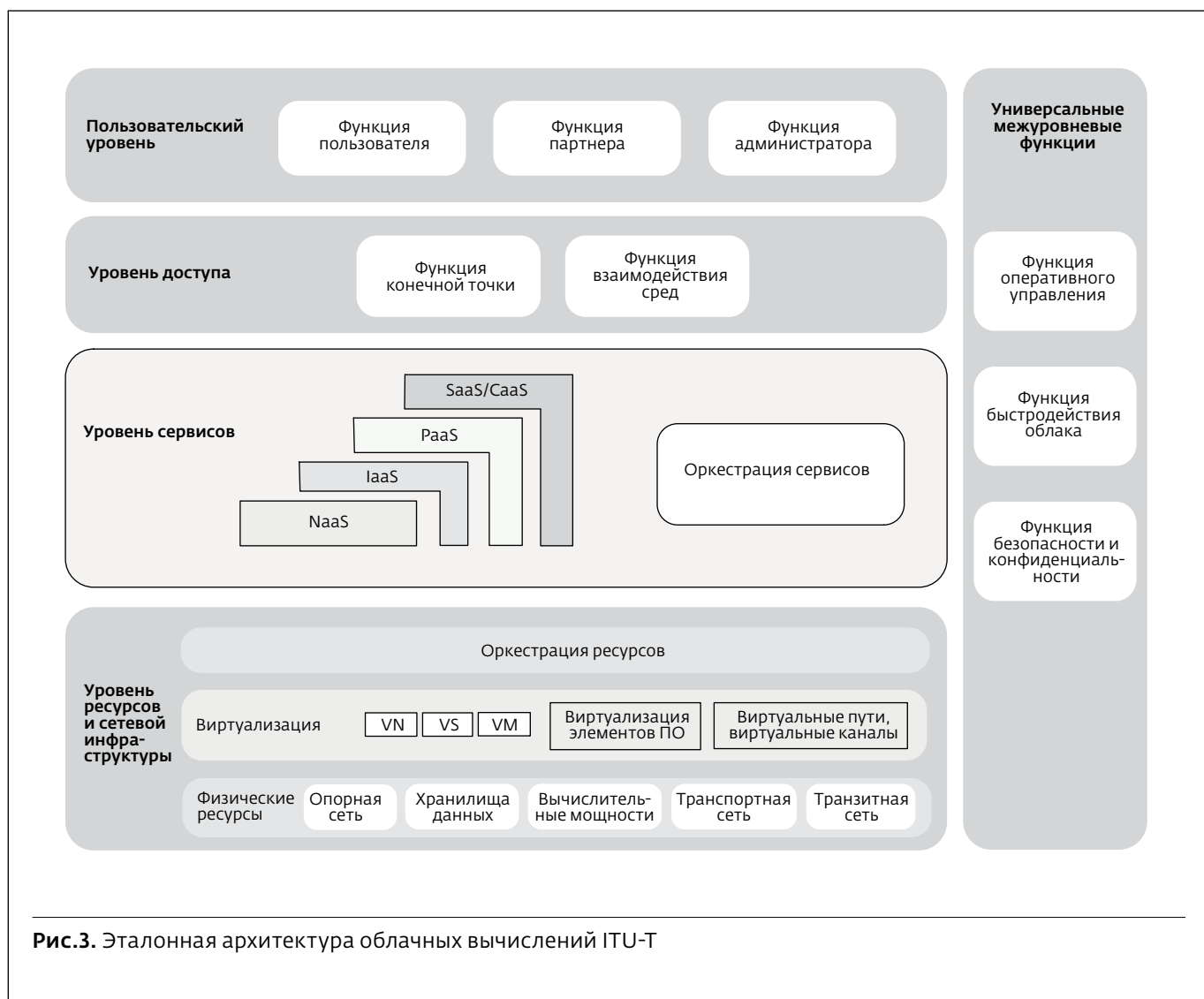


Рис.3. Эталонная архитектура облачных вычислений ITU-T

программного обеспечения, базы данных и другие компоненты ПО. Для IaaS провайдер приобретает физические вычислительные ресурсы, лежащие в основе услуги, включая серверы, сети, хранилища и инфраструктуру хостинга. Провайдер занимается оркестрацией сервисов (Service Orchestration), в рамках которой обеспечивает систематизацию, координацию и управление облачной инфраструктурой для всестороннего облачного обслуживания и согласует бизнес и ИТ-требования. Обобщенная облачная среда, которой владеет провайдер, содержит три концептуальных уровня.

На уровне сервиса (Service Layer) определяются базовые услуги, предоставляемые облачным провайдером. В случае SaaS развертываемые приложения предполагают работу с ними посредством обращения к облаку из специально

предназначенных программных клиентов и других программ конечных пользователей. В случае PaaS сервисы предназначены для разработки и развертывания приложений на облачной инфраструктуре, включая контейнеры приложений, инструменты разработки приложений, системы управления базами данных и т.п. В случае IaaS это предоставление вычислительных мощностей, систем хранения, сетевых и других фундаментальных вычислительных ресурсов, поверх которых облачные потребители могут развертывать и выполнять приложения на облачной инфраструктуре.

Уровень абстракции и контроля ресурсов (Resource Abstraction and Control Level) назначает и предоставляет элементы ПО, такие как гипервизор, виртуальные хранилища данных и поддерживающие программные компоненты,

используемые для реализации облачной инфраструктуры, поверх которой может быть определен или установлен облачный сервис. На этом уровне применяется технология виртуальных машин и/или другие формы абстракции ПО для обеспечения так называемой готовности к облаку (Cloud Readiness).

На уровне **физических ресурсов (Physical Resource Level)** размещены физические ресурсы, включая компьютерное оборудование (процессоры, память), средства хранения (жесткие диски), сетевое оборудование (роутеры, сетевые экраны, коммутаторы, интерфейсы), а также инженерная инфраструктура (Facilities) с системами кондиционирования, питания и пр.

Облачный оператор обеспечивает связь и перенос облачных сервисов от провайдера к пользователям облачных вычислений. Как правило, провайдер устанавливает SLA для предоставления услуги, что может потребовать от него совместимых с уровнем SLA предлагаемых пользователям облачных вычислений, и может потребовать от облачного оператора организации выделенных и/или безопасных соединений между облачными провайдером и пользователями.

Облачный брокер управляет использованием, производительностью и доставкой облачных сервисов, а также ведет переговоры о взаимоотношениях между провайдером и облачными пользователями. Облачный брокер полезен, когда облачные сервисы слишком сложны для того, чтобы облачный пользователь мог легко ими управлять. Облачные брокеры могут предлагать услуги с добавленной стоимостью, такие как агрегирование услуг с соответствующей отчетностью, управление идентификацией, сведениями о производительности, повышенной безопасности. Брокер может объединять несколько облачных сервисов, которые предоставляются разными облачными провайдерами, оптимизировать производительность или минимизировать затраты за счет гибкости в выборе услуг от нескольких разных облачных провайдеров.

Облачный аудитор проводит независимую оценку (Assessment) облачных сервисов, информационных систем, производительности (Performance), конфиденциальности (Confidentiality), приватности (Privacy) и безопасности (Security) реализации облака. Аудитор является независимым субъектом, который может гарантировать, что облачный сервис соответствует набору стандартов.

Следует отметить, что взаимодействие акторов облачного сервиса в рамках приведенной архитектуры может происходить разными путями. Облачный пользователь может запрашивать облачные сервисы от провайдера напрямую или через брокера. То есть один из этих пяти акторов – облачный брокер – опционален, поскольку потребители облачных сервисов (Cloud Consumers) могут получать услуги напрямую от облачного провайдера. Облачный аудитор в любом случае проводит независимые аудиты и может связаться с другими акторами для сбора необходимой информации.

Эталонная архитектура ITU-T

Несколько отличающаяся от архитектуры NIST облачная четырехуровневая эталонная архитектура предложена в разработанной 13-й Исследовательской комиссией ITU-T Рекомендации Y.3502 (рис.3).

Пользовательский уровень представляет собой интерфейс, через который клиент или партнер облачного сервиса взаимодействует с провайдером облачных сервисов и облачными службами, выполняет административные действия и контролирует облачные сервисы.

Уровень доступа обеспечивает доступ к возможностям уровня сервисов, включая как возможности самих сервисов, так и возможности администрирования и бизнес-модели с соответствующими безопасностью и QoS. Уровень доступа отвечает за представление облачных сервисов, например как набора веб-страниц, доступных через браузер, или как набора веб-сервисов с программным доступом.

Сервисный уровень содержит сами сервисы, предоставляемые провайдером облачных сервисов (SaaS, PaaS, IaaS), содержит программные компоненты, которые реализуют сервисы (но не лежащие в их основе операционные системы, драйверы устройств и т.п.) и управляет ими.

Уровень ресурсов состоит из физических ресурсов облачного провайдера и соответствующих механизмов абстракции и управления, обеспечивающих, например, виртуальную сеть, виртуальное хранилище и возможности виртуальной машины. Он также содержит функциональные возможности сетевой инфраструктуры облаков, которые необходимы для обеспечения базовой сетевой связи между провайдером и пользователями.

Кросс-уровневые функции включают в себя ряд функциональных компонентов, которые взаимодействуют с функциональными компонентами четырех других слоев для поддержки их

функционирования и взаимодействия. В число этих функций входят пять категорий компонентов: интеграция отвечает за создание единой архитектуры, обеспечивает механизмы маршрутизации сообщений и обмена сообщениями в облачной архитектуре и с внешними функциональными компонентами; система безопасности отвечает за предотвращение угроз безопасности в средах облачных вычислений (функциональные компоненты систем безопасности включают все средства безопасности, необходимые для поддержки облачных сервисов); система поддержки операций OSS охватывает набор функциональных возможностей эксплуатационного управления облачными сервисами, технического учета, системного мониторинга и фолт-менеджмента; системы поддержки бизнеса BSS включают в себя биллинг и ведение учетных записей; функция разработки поддерживает разработку облачных сервисов, компоновку, тестирование и апгрейд версий.

Следует отметить, что облачные модели подразделяются на четыре вида: частное облако, публичное, общественное и гибридное. Соответственно частное облако располагается в пределах одной организации для удовлетворения ее внутренних потребностей и гарантированной защиты от вторжений. Публичное облако предназначено для широкого доступа с простотой настройки, низкой стоимостью услуг и реализацией необходимых механизмов безопасности для контроля доступа. Общественное облако – для использования конкретным сообществом потребителей из организаций, имеющих общие задачи; оно может управляться организациями третьей стороны и существовать как внутри, так и вне юрисдикции владельца. Гибридное облако представляет собой композицию из двух или более типов облаков, когда, к примеру, бизнес-критичные приложения запускаются в приватном облаке, в то время как остальные приложения работают в публичном.

Дальнейшему развитию облачных технологий в РФ способствует принятое на государственном уровне решение о развитии цифровой экономики, предполагающее широкое использование различных облачных сервисов. По оценкам компании Huawei, за последний год рост облачных предложений достиг 25%, в то время как рынок классической ИТ-инфраструктуры вырос лишь на несколько процентов. Вот такой "клаудизм", постепенно заменяющий собой все, что мы подразумевали когда-то под словом "связь". ■