№19
Ноябрь 2023

indata
ФОНД РАЗВИТИЯ СЕТЕВЫХ ТЕХНОЛОГИЙ «ИНДАТА»

Интернет изнутри

ОБЛАЧНЫЕ ПЛАТФОРМЫ

Содержание:

Сетевое издание
Журнал **«Интернет изнутри»**
info@internetinside.ru

Выпуск №19, дата выхода:
Ноябрь 2023 г.

Свидетельство о регистрации СМИ в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций.
Регистрационный номер:
ЭЛ № ФС 77 - 85232 от 25.04.2023
ISSN: 2949-1967

Все статьи размещаются и индексируются в НЭБ eLIBRARY.RU

Издатель:
Фонд развития сетевых технологий «ИнДата»

Главный редактор:
Алексей Платонов

Выпускающий редактор:
Ирина Пыжова

Редакционная коллегия:
Елена Воронина
Марат Биктимиров

Продакшн:
Алексей Гончаров

Дизайн и вёрстка:
Дмитрий Ивлянов

Корректор:
Наталья Рябова

Обложка разработана с использованием ресурсов сайта Freepik.com

Там, за облаками...

Дорогой читатель,
Облачные услуги сегодня являются необходимым ингредиентом успешно развивающегося бизнеса. Серверы, локально исполняемые приложения, сетевая инфраструктура и даже центры обработки данных теряют свое бывшее значение и постепенно поглощаются облачными технологиями. И хотя само название вызывает ассоциации с чем-то неосязаемым, изменчивым и в то же время вездесущим, мы знаем, что облачные услуги позволили совершить существенный прорыв в области безопасности, масштабирования, производительности и эффективности использования IT-ресурсов. И все же – что же там скрывается за облаками?

В этом номере мы познакомим вас с различными аспектами облачных технологий и услуг.

Начнем с тенденций развития. Антон Салов в статье «Облачные технологии и модели: от SaaS к EDGE» анализирует развитие рынка облачных услуг и, в частности, российского рынка. Облачные технологии стремительно развиваются, создавая новые модели предоставляемых услуг, разрастаясь вширь и вглубь и проникая даже во внутреннюю инфраструктуру.

О тенденциях российского рынка «новой нефти» и его стремительном росте рассказывает Алексей Костин.

О развитии облачных платформ в другом измерении – в космосе – пишет Владимир Глебский. И это не фантазия – гиганты облачной индустрии развертывают мощные «заоблачные» проекты.

Билгин Ибрям представляет тенденции эволюции облачных вычислений с точки зрения технологического развития. В статье «Эволюция облачных вычислений: от сырой инфраструктуры к облаку бессерверных приложений» он последовательно рассматривает историю этих технологий, начиная с «сырого металла».

Облака обычно ассоциируются с высоким уровнем централизации управления. Хотя облачные платформы географически распределены, их организация и управление сосредоточены в руках провайдера этих услуг. В статье «Децентрализация облаков в общем тренде развития IT-индустрии» Марат Биктимиров размышляет, как децентрализованные подходы могут улучшить масштабируемость, устойчивость и безопасность.

И если вы думаете, что облака – это сложно, читайте анализ Александра Венедюхина, который рассказывает, как технологии туннелирования на основе DoH и шифрования приводят к усложнению базовой инфраструктуры Интернета и кардинальному изменению его ландшафта.

Мы продолжаем публиковать статьи в новом разделе «Интернет-наука и образование». В этом номере группа авторов описывает метод сквозной аутентификации пользователей в системе поддержки проведения научно-технических экспертиз.

Ну и конечно мы продолжаем поддерживать наши стандартные разделы. В разделе «Политика» Мадина Касенова предлагает анализ усилий Евросоюза, направленных на обретение цифрового суверенитета. А в «Новостях» мы познакомим вас с интересными фактами Интернета и доменной индустрии.

Как всегда, нам очень интересно и важно знать ваше мнение. Что понравилось и что можно улучшить? Какие темы вы хотели бы увидеть в следующих выпусках? Пишите нам по адресу info@internetinside.ru.

Редакция журнала

Облачные технологии и модели: от SaaS к EDGE

Антон Салов

Российский облачный рынок начал активно развиваться в конце 2000-х годов, и этот период ознаменовался рождением первых стартапов, специализирующихся на предоставлении услуг SaaS (программное обеспечение как услуга). Среди них можно выделить такие компании, как Asoft, «Мегаплан», «МойСклад», которые стали пионерами в этой области. Параллельно с развитием SaaS-проектов появились и другие инновационные инициативы, например, проекты по автоматизации бухгалтерской отчетности, такие как «СКБ Контур» и «Калуга Астрал», сервис проведения онлайн-конференций «Вебинар». Они значительно упрощали повседневные задачи бизнеса, предоставляя возможность решать их без необходимости установки программ на персональные компьютеры, просто с использованием веб-браузера.

Собственно, облачная модель предоставления тех или иных услуг практикуется уже много лет. Основными моделями являются SaaS (Software as a Service) — это облачная модель предоставления программного обеспечения, PaaS (Platform as a Service, платформа как услуга) — это способ предоставления вычислительных ресурсов в облаке, когда пользователь получает уже готовый сервис или платформу для запуска своего кода и хранения данных, и IaaS (Infrastructure as a Service, инфраструктура как услуга) — модель, по которой потребителям предоставляются по подписке фундаментальные информационно-технологические ресурсы — виртуальные серверы с заданной вычислительной мощностью, операционной системой и доступом к сети. Существует интересное и популярное разъяснение разницы между этими моделями, которое выглядит так: «IaaS — корова в аренду, PaaS — молокозавод, а SaaS — молоко в супермаркете».

Особую эффективность облачные сервисы показывали не только там, где они заменяли традиционное программное обеспечение, но и там, где они позволяли заменять оборудование – в коммуникационной сфере, заменяя железную АТС на виртуальную (ВАТС) или сервер видеоконференций (ВКС) – такой как Polycom или Cisco – на облачный сервис того же «Вебинара». Уже тогда они делали доступной связь для малого и среднего бизнеса, а сейчас, после пандемии Covid-19 и вхождения (похоже, что необратимого) в нашу жизнь «удалёнки», даже крупный бизнес не представляет своих процессов без таких сервисов.

В России насчитывается порядка 10 различных сервисов облачных видеоконференций. Большинство из них появились в последние несколько лет, когда каждая крупная цифровая компания считала своим долгом написать еще одну российскую ВКС. Все они очень похожи по своей функциональности просто потому, что никто не стал заморачиваться и писать с нуля свою систему ВКС, а брал за основу популярные open source-проекты вроде Jitsi. Jitsi — это набор бесплатных и открытых мультиплатформенных приложений для голосовой связи, видеоконференций и мгновенных сообщений для веба и клиентов популярных операционных систем.

Вопрос, конечно же, не только в функциональности облачных систем видеоконференций. Именно в пандемию резко возросло число пользователей таких сервисов и, соответственно, нагрузка на облачную инфраструктуру. Например, сейчас многим клиентам требуется возможность одномоментно подключать к вещанию тысячи пользователей — и тот же «Вебинар» вполне справляется с подобными нагрузками.

Рынок SaaS в России долгие годы формировали в основном зарубежные игроки, такие как Microsoft, Google, Atlassian, Zoom, а также упомянутые выше российские стартапы. Если смотреть на структуру всего российского рынка облачных услуг, то до начала цифровизации и роста доверия к облачной модели со стороны крупного бизнеса SaaS занимал порядка 2/3 всего рынка. Рост спроса на IaaS/PaaS в последние пять лет уменьшил рыночную долю SaaS до 50%. А по итогам 2022 года темпы роста рынка SaaS сократились практически до нуля, а по оценкам ряда экспертов сам сегмент даже несколько сократился. Это связано с тем, что зарубежные игроки ушли с российского рынка, а заместить все их сервисы в моменте довольно сложно: это не просто инфраструктура, а программное обеспечение, которое много лет писали команды разработчиков глобальных компаний, и для ряда инструментов на сегодняшний день очевидной замены не существует, хотя ее активно ищут.

С другой стороны, уход ряда западных игроков с российского рынка за последние два года, рост спроса на импортозамещение – это ключевые факторы ренессанса в российском SaaS-сегменте. Российские SaaS-компании показывают стабильный рост и активно решают проблемы российского бизнеса.

Но давайте перейдём от SaaS к инфраструктуре, которая развёрнута под ним.

IDC (International Data Corporation) опубликовала отчет по глобальному рынку инфраструктурных облаков. Несмотря на сложную геополитическую обстановку, макроэкономические вызовы и высокую инфляцию, аналитики считают, что отрасль будет продолжать стабильно расти.

По их данным расходы на публичный IaaS будут демонстрировать CAGR (Compound Annual Growth Rate, среднегодовые темпы роста) на уровне 11,6%, и к 2027 году их объем достигнет $109,7 миллиарда. Это будет составлять примерно 70% от общего объема инвестиций в облачные платформы. В то время как в сегменте частных облаков прогнозируется более низкий CAGR в размере 10,7%, и его предполагаемый объем составит $47,0 миллиарда к концу прогнозируемого периода [1].

А что же у нас?

В части инфраструктурных облаков развитие российского рынка началось несколько позже и с существенным отставанием от США и Европы, где уже с начала 2000-х начал формироваться новый способ предоставления IT-услуг. Этот подход получил название MSP (Managed Service Provider), он охватывает не только облачные услуги, но и другие виды IT-сервисов. Именно в этот период начали появляться провайдеры, предоставляющие профессиональную облачную инфраструктуру на базе коммерческих дата-центров. Они использовали MSP-лицензии от вендоров, таких как VMware и Microsoft, для построения своей инфраструктуры и предлагали основные услуги, такие как хостинг виртуальных машин и хранилища данных. А параллельно начал формироваться рынок гиперскейлеров – таких как Amazon Web Services (AWS) и Microsoft Azure, которые создавали услуги не только класса IaaS, но и PaaS.

В России в начале прошлого десятилетия развитие IaaS пошло в двух направлениях. Первое – перепродажа услуг зарубежных провайдеров и гиперскейлеров с рядом сопутствующих услуг вроде помощи в миграции, техподдержке и биллинге. Этим направлением занимались российские дистрибьюторы и интеграторы. Направление успешно развивалось до середины 2022 года и вносило весомый вклад в российский облачный рынок. Второе – создание собственной облачной инфраструктуры в коммерческих ЦОД. В этом направлении сначала начали работать вчерашние хостеры и системные интеграторы, позже в гонку включились операторы связи, банки и сами поставщики услуг ЦОД.

Лидирующим стеком построения облаков для корпоративного сектора долгое время оставался VMware, тогда как облака для веб-нагрузок строили на базе KVM/OpenStack. Это определялось тем, что корпоративные клиенты для внутренних нагрузок использовали виртуализацию VMware и не хотели менять привычный стек при миграции в облако, поэтому они просили интеграторов использовать ту же платформу. VMware изначально предлагала очень качественные решения и для корпоративной виртуализации, и панели управления для облаков. Кроме того, некоторые провайдеры писали поверх вендорской панели управления свою собственную, потому что это давало большую гибкость и лучше соответствовало запросам клиентов. Однако помимо управления облакам нужен еще и биллинг.

С точки зрения тарификации и биллинга IaaS представляет собой более сложный тип сервисов, чем SaaS. Конечная стоимость услуги зависит в среднем от пяти-шести параметров, которые в течение отчетного периода изменяются, тогда как у большинства SaaS тарификация зависит от числа пользователей и/или двух-трех типов функциональных возможностей, объединенных в тарифные планы. Это, кстати, роднит облака с услугами операторов связи, где конечному клиенту также предлагается комплексный тарифный план с набором включенных минут, SMS и Гб. Помимо фиксированных тарифных планов, в инфраструктурных облаках предлагается тарификация по принципу pay-as-you-go – с оплатой за фактическое потребление, когда стоимость единицы ресурса существенно выше, чем стоимость этой же единицы в комплексном тарифе, но появляется возможность гибкого подхода к нагрузке. В связи с этим на рынке появился отдельный класс систем – облачные биллинги, которые были востребованы у начинающих провайдеров, так как существенно упрощали выход на рынок.

В период пандемии крупный бизнес активно выносил нагрузки в облако, чтобы обеспечить работоспособность и непрерывность процессов. Но спрос рос неравномерно. Несмотря на увеличение спроса на облачные ресурсы в некоторых отраслях, в других отраслях наблюдается стагнация, что привело к снижению потребления информационных технологий, включая облачные вычисления. Однако в целом бизнес стал больше доверять облакам, а спрос на цифровую трансформацию подтолкнул к использованию не только простого IaaS, но и контейнерной виртуализации и элементов PaaS, таких как искусственный интеллект, машинное обучение, аналитика

данных и блокчейн-технологии. Разработчики и предприниматели получили доступ к широкому спектру инструментов и сервисов, предоставляемых облачными провайдерами. Они включают в себя базы данных, хранилища данных, DevOps-инструменты, мониторинг и управление, а также инструменты для разработки и развертывания приложений. Использование такой экосистемы облачных продуктов упрощает процесс разработки и сокращает затраты на этапе создания цифровых продуктов.

Упомянутая выше контейнерная виртуализация представляет собой важное инфраструктурное направление у большинства современных российских провайдеров. Контейнерная виртуализация — это методология построения облачной инфраструктуры, которая позволяет упаковывать приложения и их зависимости в контейнеры, которые могут быть запущены и работать в изолированном окружении. Например, Google использует свою платформу для запуска миллионов контейнеров каждую неделю. Инженеры компании, собственно, и создали в середине прошлого десятилетия систему управления контейнерами Kubernetes, которая стала стандартом в отрасли.

Контейнеры, по сути, это миниатюрные виртуальные машины, которые обеспечивают внутри себя все необходимое для функционирования приложения: операционную систему, библиотеки, исполняемые файлы и конфигурационные настройки. Однако в отличие от традиционных виртуальных машин, контейнеры более легковесны и, как следствие, на одном и том же оборудовании их можно разместить более плотно, чем классические виртуальные машины. Контейнеры могут быть развернуты практически везде, где есть поддержка контейнерной виртуализации, вне зависимости от операционной системы или инфраструктуры. Это позволяет разработчикам создавать приложения, которые легко могут быть перенесены между разными средами – разрабатывать приложение можно на ПК, а потом запускать его на промышленном компьютере или даже роутере. К другим преимуществам контейнеров можно отнести то, что с их помощью разработчики могут точно определить окружение, в котором будет работать их приложение. Это позволяет избегать конфликтов между зависимостями и облегчает управление версиями. Также стоит отметить, что контейнеры идеально подходят для микросервисных приложений, позволяя каждому сервису работать в своем собственном контейнере, что способствует легкости сопровождения и разработки масштабируемых систем. А микросервисы, в свою очередь, это ключевой тренд архитектуры современных cloud ready-систем. Эта технология помогает компаниям быстро адаптироваться к изменяющимся рыночным условиям и сокращать время от идеи до релиза. С развитием инфраструктуры и инструментов для контейнерной виртуализации она становится незаменимой частью современной разработки программного обеспечения.

И всё же вернемся пока к классической виртуализации в облачной инфраструктуре. В 2022 году ряд вендоров популярных систем виртуализации и управления облаками покинули Россию, как ушли и зарубежные провайдеры и гиперскейлеры. Согласно данным экспертов RCCPA, до 2022 года зарубежные провайдеры составляли порядка 30% общего прироста объема облачного рынка в России. Основной вклад в этот прирост внесли компании Microsoft и AWS, а также VMware, предоставляющие программное обеспечение для провайдеров и внутренней виртуализации. Уход зарубежных провайдеров вылился во взрывной рост спроса на российскую облачную инфраструктуру. При этом российские провайдеры с радостью были готовы принять новых клиентов, не забывая повышать цены, а клиенты имели возможность переносить свои приложения и данные в привычное окружение VMware, поскольку многие провайдеры продолжают предоставлять свои услуги на основе этой платформы, даже если у нее отсутствует официальная поддержка от производителя. С другой стороны, некоторые крупные облачные поставщики готовы предоставить услуги по миграции на KVM, иногда даже бесплатно.

Параллельно многие провайдеры начали задумываться о том, как развиваться дальше. Далеко не у всех была своя импортозамещенная платформа для построения облаков. К тому же, потеряв поддержку от зарубежных вендоров, провайдеры потеряли и обновления, включая критичные обновления безопасности.

Ряд провайдеров до сих пор занимает выжидательную позицию, ожидая возвращения западных вендоров – как ушли, так и вернутся. В качестве временного решения можно воспользоваться возможностью не платить отчисления за ПО, а за технической поддержкой обратиться к российским интеграторам, которые забрали многих сотрудников той же VMware.

Другой вариант – переход на собственное решение или решение на базе открытого кода – тот же OpenStack. Преимущество этого подхода заключается в том, что не нужно платить сторонним организациям. Оборотная сторона – требуется наличие собственной команды разработчиков или хорошо подготовленных специалистов по открытым решениям (либо можно купить команду, которая умеет готовить OpenStack). Этот вариант приемлем для крупных провайдеров с большим штатом разработчиков.

И третий путь – переход на решение по виртуализации от российского вендора. В едином реестре российских программ для ЭВМ и баз данных (ЕРРП) в 2023 году представлен широкий спектр инфраструктурных решений по виртуализации, в том числе облачные и гиперконвергентные платформы. Но не все они подходят для оказания облачных услуг, также не решен и ключевой вопрос – где взять специалистов, умеющих работать с новыми платформами. На российском рынке труда много специалистов по VMware, но очень мало свободных инженеров, которые умеют работать с OpenStack. Причина очевидна: у нас на рынке и до 2022 года было три крупных провайдера, использующих OpenStack, и они «скупали на корню» всю экспертизу, и в первую очередь специалистов по российской виртуализации. Для решения этой непростой задачи некоторые вендоры активно развивают свои и партнерские тренинг-центры, некоторые продают свою экспертизу, а некоторые подошли к этому вопросу еще более изобретательно. Нет специалистов по нашему продукту, но есть специалисты по VMware? Так мы будем развивать интерфейсы нашего продукта, чтобы они были максимально близки к аналогичным продуктам VMware, вплоть до расположения кнопок. Крайне интересная стратегия, которая на глобальном рынке могла бы быть сопряжена с исками от VMware, но в текущих условиях об этом можно не беспокоиться.

Об эволюции моделей облачных услуг

С ростом спроса на цифровую трансформацию, то есть создание цифровых продуктов средним и крупным бизнесом, и с выносом чувствительных данных в облака (те же внутрикорпоративные системы) в мире и в России отчетливо наметился тренд на применение гибридных и мультиоблачных стратегий.

Гибридное облако (Hybrid Cloud) — это облачная компьютерная инфраструктура, которая объединяет в себе элементы двух или более типов облачных вычислений: публичных облаков (public cloud), частных облаков (private cloud) и, иногда, локальных инфраструктурных ресурсов (on-premises) или выделенных серверов (bare metal cloud).

Bare Metal Cloud (или выделенное оборудование в облаке) представляет собой эволюцию облачных вычислений, которая позволяет арендовать выделенное физическое оборудование, такое как серверы, без необходимости виртуализации. Одной из ключевых особенностей Bare Metal Cloud является высокая производительность. Поскольку пользователи имеют полный доступ к физическому оборудованию, они могут оптимизировать его конфигурацию под свои потребности, что позволяет достичь максимальной производительности при выполнении вычислительных задач. Пользователи Bare Metal Cloud имеют гарантированный доступ к ресурсам, без соседей на одном физическом сервере, что обеспечивает предсказуемость работы приложений. Это особенно важно для приложений, требующих стабильности и непрерывной доступности. А поскольку нет виртуализации, снижается риск утечки данных между виртуальными машинами. На физическом сервере нет соседних виртуальных машин, что уменьшает риск шума соседей и повышает безопасность данных, а потенциальные атаки, эксплуатирующие уязвимости класса Spectre/Meltdown/TLBleed из виртуальных сред, обычно не применимы.

Гибридные облака могут быть настроены по-разному в зависимости от потребностей конкретной организации. Это может включать в себя развертывание приложений в частных облаках, а резервное копирование данных в публичные облака, создание гибридных мостов для обмена данными между разными облаками и многое другое. Главное преимущество гибридных облаков заключается в том, что они предоставляют компаниям большую гибкость и контроль над их IT-средой, что в свою очередь позволяет им лучше соответствовать своим бизнес-потребностям и требованиям безопасности. Важность обеспечения безопасности данных и соблюдения законодательных норм и регуляций становится все более критической. Гибридные облака позволяют удовлетворить эти требования, предоставляя более чёткий контроль над данными и уровнем безопасности.

Мультиоблако (Multicloud) — это стратегия использования облаков от нескольких облачных провайдеров для удовлетворения вычислительных потребностей организации. Реализуя мультиоблачную стратегию, компании могут одновременно использовать услуги и ресурсы нескольких облаков, таких как публичные облака, частные облака и гибридные облака. Но в отличие от гибридных облаков, здесь всегда присутствуют несколько провайдеров, что позволяет экономить при общей гибкости решения, но накладывает обязательство по решению задачи управления мультиоблачными средами. Это может быть сложным и требует хорошей координации и интеграции разных облачных платформ, биллингов, систем разграничения прав доступа. Решать эту задачу можно в ручном режиме, сводя биллинг на уровне финансов, или же через платформу-оркестратор или платформу-брокер, которая позволяет командам заказывать услуги от различных поставщиков в едином интерфейсе и с единым биллингом. Это крайне удобно, когда в рамках создания цифровых продуктов компания приобретает, к примеру, платформенные сервисы DataOps или MLOps у гиперскейлера, упрощая процесс разработки, и параллельно для продуктивной среды берёт Bare Metal у другого поставщика. В связи с дефицитом ряда типов оборудования, который сложился в последние два года из-за ограничения поставок, мультиоблачная стратегия является выигрышной – если в данный момент нельзя взять GPU-хостинг (специализированный тип облака, с мощными графическими картами, используемый в том числе и в задачах ИИ) у одного провайдера, то его можно взять у другого, чьи ресурсы свободны. Внутреннему клиенту, который решает свою задачу, может быть непринципиально, в каком ЦОД и от какого поставщика он получит виртуальную машину с требуемыми параметрами. Мультиоблачный поход позволяет бизнесу оптимизировать расходы на облачные услуги, выбирая наилучшие решения и провайдеров для конкретных задач.

Но, безусловно, у такой модели есть плюсы и минусы, и IT-департамент вместе с IT-директором должны иметь четкую стратегию и план управления мультиоблаками, чтобы обеспечить эффективное использование всех выбранных облачных платформ.

Еще один важный аспект, который стоит отметить: гибридные и мультиоблачные стратегии обеспечивают сравнительно высокую доступность данных и приложений для бизнеса, который оперирует приложениями и данными в разных регионах. Это особенно важно для глобальных компаний, так как в разных регионах и странах разное законодательство, которое может


Изображение от Freepik

их создания. В промышленном контексте это могут быть датчики, контроллеры, роботы и другие устройства, используемые на производственных линиях. Главное преимущество EDGE-вычислений заключается в том, что они позволяют обрабатывать данные на месте, минимизируя задержки и потребление сетевых ресурсов.

В EDGE-модели на предприятии может быть развёрнут EDGE-узел (EDGE Node, система серверов и СХД), который способен собирать и обрабатывать информацию изолированно от внешнего ЦОД провайдера, используя те же контейнеры. А вот за жизнеспособность контейнерной виртуализации на EDGE следит уже провайдер, и в случае, если EDGE-узлу не хватает ресурсов, например, для создания резервных копий, то их можно будет передать в централизованный ЦОД провайдера. При этом то, какие данные можно отдавать «наружу», определяет сама IT-служба предприятия.

определять политику по тем же персональным данным. Сейчас, когда ряд провайдеров разделяет бизнес на российский и зарубежный, изолируя, в том числе и на уровне доступных локаций, ЦОД, а другие провайдеры, наоборот, открывают новые локации в Средней Азии или на Ближнем Востоке, мультиоблачный подход прочно вошел в жизнь тех же поставщиков SaaS и других цифровых продуктов.

От облачных вычислений к граничным

Мы рассмотрели, как облака помогают изменять подходы к внутрикорпоративной инфраструктуре, к внутренним IT-процессам компании, а также становятся движителем цифровизации. Однако ключевой задачей облаков и облачных провайдеров на ближайшие годы будет являться поиск своего места в реальном секторе экономики. То есть им предстоит понять, каким образом они могут прийти на завод или к сельхозпроизводителю, чтобы помочь создать ценность для производственного процесса, как повысить эффективность, управляемость и снизить издержки. Завод и сельское хозяйство приведены в качестве примеров неспроста, так как в отличие от компании, которая располагается в городском офисе, в данных случаях сетевая связанность с ЦОД провайдера может оказаться под вопросом. Данные в тех же SCADA-системах (системы управления производственными процессами) критичны к задержкам, и их нельзя выносить во внешний ЦОД, который расположен за десятки и сотни километров. Массивы информации со множества IIoT-датчиков (сенсоры промышленного Интернета вещей), установленных на станках и конвейерах, передаются в реальном времени в SCADA. При этом требования к безопасности на производстве куда выше, и многие промышленные предприятия не горят желанием выносить свои данные за периметр, опасаясь утечек, атак и промышленного шпионажа. И тут на помощь приходят EDGE-вычисления.

EDGE-вычисления – разновидность облачных моделей, которая позволяет обрабатывать данные и выполнять вычисления непосредственно на устройствах, находящихся близко к месту

EDGE-вычисления позволяют проводить мониторинг состояния оборудования в реальном времени: с помощью IoT-датчиков и аналитики данных на месте можно выявлять отклонения и предсказывать отказы оборудования, что позволяет устранять неполадки до их серьезного воздействия на производственный процесс. Параллельно EDGE позволяет анализировать данные с производственных линий и принимать решения на основе этой аналитики в реальном времени, что может включать в себя оптимизацию производственных параметров, планирование производства и управление запасами.

Промышленное производство — одна из областей, которая постоянно стремится к повышению эффективности и улучшению производственных процессов. В этом контексте технологии EDGE-вычислений становятся все более значимыми и позволяют компаниям решать сложные задачи в реальном времени, улучшать безопасность и экономичность производства, а также снижать потребление энергии и ресурсов.

За последние 15 лет рынок облачных услуг претерпел значительные изменения, которые существенно повлияли на бизнесы, потребителей и технологический ландшафт в целом. Облачные технологии стали неотъемлемой частью современного мира, предоставляя огромное количество возможностей для хранения данных, разработки приложений и продуктивных коммуникаций. Мы рассмотрели лишь небольшую часть тех трансформаций, которым подверглись модели предоставления облачных услуг в мире и в России, а также их влияние на бизнес, производство и нашу жизнь.

Литература

Cloud Infrastructure Spending Continued to Grow in the Second Quarter of 2023 Led by Spending on Shared Cloud Infrastructure, According to IDC Tracker, https://www.idc.com/getdoc.jsp?containerId=prUS51280423

Об авторе:

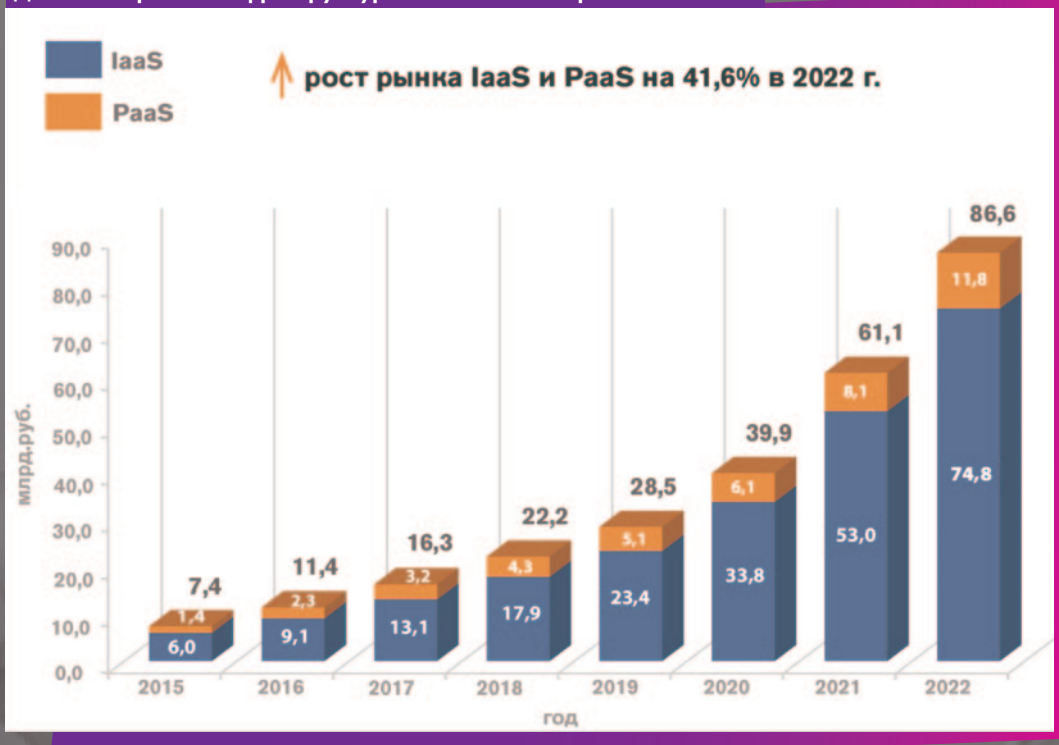
Антон Салов, член оргкомитета Russian Cloud Computing Professional Association (RCCPA)

Интернет в цифрах

Технологические тренды 2023 года

Источник: Gartner.com (https://www.gartner.com/en/articles/gartner-top-10-strategic-technology-trends-for-2023)

Динамика рынка инфраструктурных облачных сервисов в России



Источник: iKS-Consulting (http://survey.iksconsulting.ru/page32257739.html)

Тенденции развития облачных вычислений

Источник: The Future of Commerce (https://www.the-future-of-commerce.com/2022/11/09/cloud-computing-trends-2023/)

Эволюция облачных вычислений: от «сырой» инфраструктуры к облаку бессерверных приложений

Билгин Ибрям

Облачные вычисления постепенно превращают весь комплекс программного обеспечения, за исключением бизнес-логики, в продукт. Все началось с «сырой» инфраструктуры, но облачные технологии теперь движутся выше по стеку — к уровню приложений. Эволюция облачных технологий меняет способы внедрения и эксплуатации приложений. Если ранее монолитные приложения, в прошлом отвечавшие за все аспекты распределенного приложения, постепенно преобразовывались в контейнерные микросервисы и функции, управляемые платформой, то теперь они полностью смешиваются с облачными сервисами и делегируют им управляющую логику.

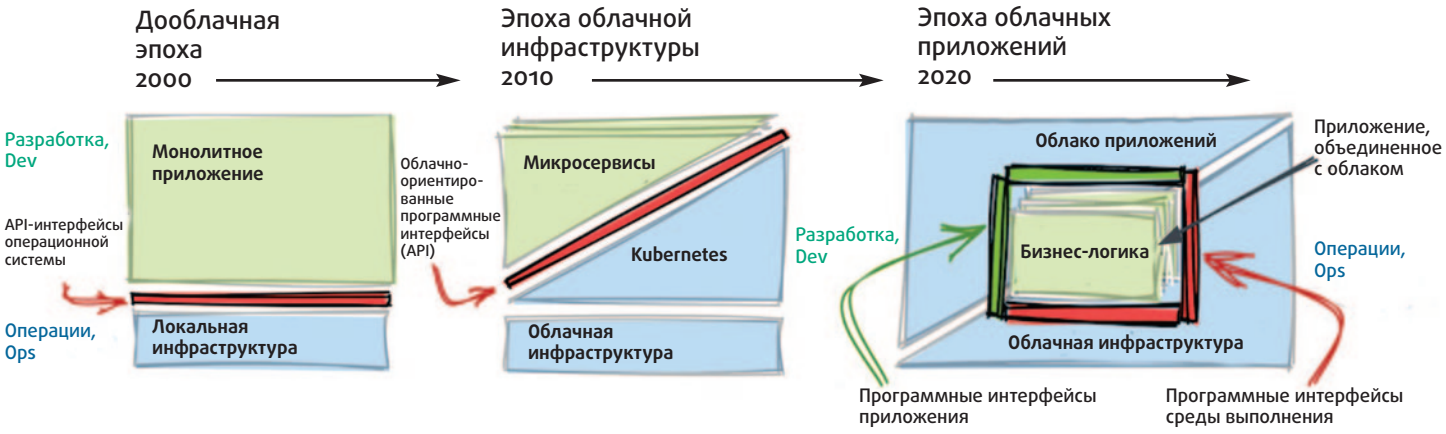


Рис. 1. Облачные вычисления, превращающие стек приложений в продукт.

В данной статье мы рассмотрим основные этапы эволюции, характеризующиеся присущими им тенденциями развития инфраструктуры и архитектуры приложений, а также выполняемыми функциями. Для наглядности мы будем использовать AWS (Amazon Web Services; веб-сервисы Amazon), но те же тенденции можно наблюдать и у других облачных сервисов. Также мы рассмотрим, посредством каких типов API взаимодействуют приложения и инфраструктура и как функции приложений смещаются в сторону инфраструктуры, прежде чем стать продуктом облачных сервисов.

Дооблачная эра

Это время монолитных приложений, локальных центров обработки данных и ранних облачных сервисов. Сегодня такая настройка считается устаревшей, и мы опишем ее здесь главным образом как отправную точку эволюции распределенных приложений. В этой архитектуре все распределенные процедуры выполняются внутри приложения, а сама инфраструктура обрабатывается настолько регламентировано и статично, насколько это было возможно.

Рис. 2. Дооблачная эра монолитных приложений и статической инфраструктуры.

Статическая инфраструктура

С точки зрения инфраструктуры, это время до появления Kubernetes и первых дней внедрения AWS EC2. Основной характеристикой этой эпохи является статичный характер инфраструктуры, состоявшей из больших виртуальных машин. Элементы этой инфраструктуры содержат множество приложений и даже некоторые динамические компоненты с отслеживанием состояния, такие как базы данных, брокеры сообщений и хранилища контента.

Монолитные приложения

Наилучшими представителями этой архитектуры со стороны приложения являются SOA (сервис-ориентированная архитектура) и ее реализация — Enterprise Service Bus (сервисная шина предприятия). Эти приложения имели большое монолитное развертывание, способное удовлетворить такие потребности, как:

- Развертывание в среде выполнения: новые релизы обычно упаковываются в виде библиотек и планируются к выполнению на заранее выбранных узлах с возможностью ручного отката.
- Синхронное взаимодействие: возможность обнаружения сервисов, балансировки нагрузки, повторного выполнения операции, разрыва цепи и т.д. Важно не только перераспределение трафика и пробный релиз, но и то, что новые выпуски будут выполняться за один раз для всего приложения и иметь взаимодействие с архитектурой in-memory.
- Асинхронное взаимодействие: наличие обширного ассортимента соединителей с возможностью преобразования, фильтрации и маршрутизации сообщений и событий.
- Рабочие процессы с отслеживанием состояния: основной характеристикой монолитной архитектуры является общее для всех элементов состояние, что упрощает выполнение оркестровок с отслеживанием состояния, идемпотентности, кеширования, запланированных задач и т.д.

Поскольку инфраструктура обеспечивает только вычисления, хранение и сетевое взаимодействие, стек приложений отвечал за реализацию большинства бизнес-возможностей, выполнение нефункциональных требований и процесс развертывания.

Операционная система как аппаратно-программный интерфейс

В дооблачную эру отсутствуют общие абстракции приложений и инфраструктуры, а также технологии и практики, совместно используемые командами разработчиков и операторов. Эти разрозненные команды используют операционную систему, фиксированные IP-адреса и виртуальные машины в качестве разграничения стека приложений. Операционная группа отвечает за подготовку виртуальных машин и обеспечение достаточного количества дополнительных мощностей для будущего роста приложений. Разработчики отвечают за реализацию всех аспектов распределенного приложения, работающего на этой инфраструктуре. Из-за отсутствия универсального формата пакетирования и API для развертывания и размещения каждое приложение будет выпускаться в виде уникальной коллекции библиотек с инструкциями, написанными в удобной для восприятия человеком «вики-форме», а не в виде машинного исполняемого файла, который можно воспроизвести. API, с которыми взаимодействуют приложение и инфраструктура, — это API операционной системы в виде запуска процесса, его завершения, фиксированных IP-адресов машин, а не абстракции приложений. В эпоху инфраструктурного подхода приложение является «гражданином второго сорта», и разработчикам приходится адаптировать и приспосабливать приложение к форме и интерфейсам инфраструктуры.

Эпоха инфраструктурно-центричных облаков

Это время перехода к микросервисам, хранилищам, Kubernetes и массовой миграции в облака. Данный этап характеризуется реорганизацией приложений в микросервисы, переносом жизненного цикла приложений и сетевых функций с прикладного уровня на Kubernetes и дополнительные технологии.

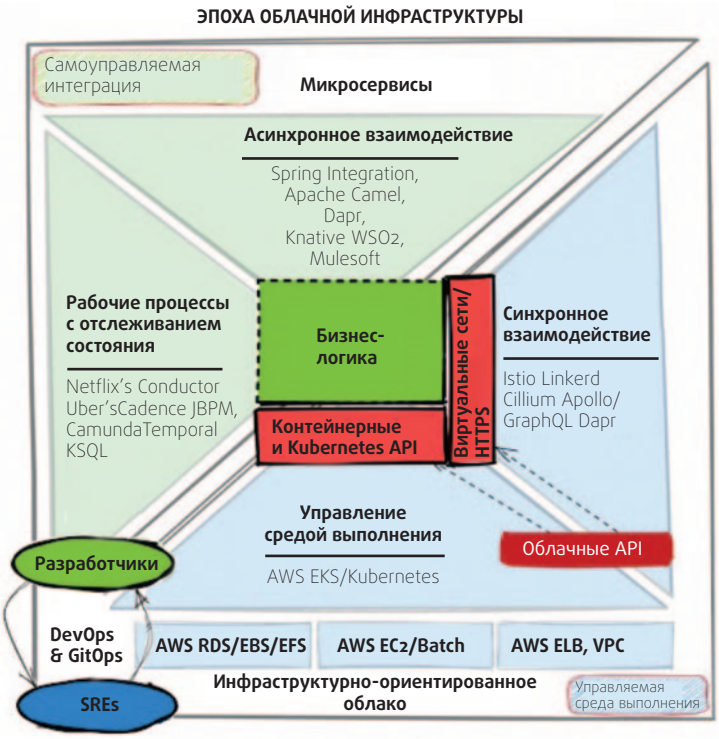


Рис. 3. Эпоха инфраструктурных облаков микросервисов и Kubernetes.

Облачно-ориентированная инфраструктура

В эту эпоху происходят два крупных инфраструктурных сдвига. Во-первых, это внедрение облачной инфраструктуры и переход на EC2, ELB, RDS и т.д. Эти облачные сервисы предлагают те же массивные инфраструктурные единицы и API, что и локальная инфраструктура, но перекладывают ответственность за управление, мониторинг, масштабируемость и надежность от внутренней операционной группы к облачным провайдерам. Вторая важная тенденция — появление контейнеров и Kubernetes, которые приводят к управляемому жизненному циклу приложений. Контейнеры обеспечили универсальный формат пакетирования, изоляции и выполнения приложений. А Kubernetes представил абстракции и декларативные API для массовой оркестровки приложений, при этом заботясь о жизненном цикле и сетевых проблемах. Благодаря этим двум скачкам исходная инфраструктура была перенесена в облако, а ответственность за жизненный цикл приложений перешла к инфраструктурным подразделениям. Давайте посмотрим, как это повлияло на прикладной уровень.

Микросервисная архитектура

Поскольку монолитные приложения распадались на независимые развертывания, первоначальные микросервисы содержали в себе слишком много инфраструктуры. С появлением контейнеров и технологий Kubernetes и Service Mesh эти обязанности были вынесены за пределы стека приложений. Проблемы жизненного цикла и развертывания, такие как тестирование работоспособности, масштабирование и конфигурирование, стали частью уровня инфраструктуры, будь то Kubernetes Pods, AWS Beanstalk или Heroku Dynos. Сетевые проблемы также вышли за рамки прикладного уровня. Обнаружение служб, балансировка нагрузки, mTLS, отказоустойчивость сети – все это начало переходить сначала к связанным приложениям, таким как Envoy, затем к агенту общего узла, такому как Ztunnel от Istio, а некоторые функции, такие как наблюдаемость и mTLS, даже дальше, в ядро Linux через eBPF и Cilium. В результате интеграция, управляемая событиями, и обязанности по рабочему процессу, влияющие на поток управления приложением и бизнес-логику, на данный момент остаются в пределах приложения и досягаемости разработчиков. Но вместо встраивания в монолитное приложение они будут развернуты как автономные промежуточные программы, некоторые из которых ориентированы на обработку событий (например, экосистема Kafka), некоторые — на отслеживание состояния (Camunda), а некоторые — на другие библиотеки, предлагающие возможности интеграции без сохранения состояния (например, Apache Camel).

Kubernetes как API

Когда необработанная инфраструктура стала продуктом, поставщики облачных услуг переключили свое внимание на уровень приложений. Контейнеры и API Kubernetes стали общепринятыми для упаковки приложений и управления жизненным циклом ресурсов. Это первый случай, когда появляется общепринятый API-интерфейс, ориентированный на приложение, который управляет жизненным циклом и сетевыми аспектами приложения, а не всей виртуальной машиной. После упаковки приложения в образ контейнера с указанием портов и проверок работоспособности приложение можно передать команде эксплуатации для масштабного запуска в виде «черного ящика» без каких-либо ручных вмешательств. Что касается сети, HTTP и REST стали нормой для синхронного взаимодействия приложений, а реализации Service Mesh использовались для управления этим трафиком с помощью функций переключения, наблюдаемости, mTLS и отказоустойчивости. Это время, когда разработчики и рабочие группы начали использовать общие инструменты и практики, такие как GitOps и DevOps, что в целом привело к улучшению сотрудничества между ними. Это означало, что существует общий API для жизненного цикла приложения и сетевых аспектов, который создает основу для следующего этапа превращения в продукт того, что осталось от прикладного уровня.

Эра облачных технологий, ориентированных на приложения

Сегодня жизненный цикл приложения и работа в сети управляются в основном прозрачно для приложения. За исключением одной или двух конечных точек работоспособности разработчикам не нужно ничего кодировать в приложении, чтобы облачная среда выполнения могла запускать, масштабировать и направлять трафик в приложение. Эти сервисы облачной среды исполнения работают прозрачно для приложения, используя абстракции на основе контейнеров для жизненного цикла и методов маршрутизации трафика HTTP/TCP. Но это не относится к аспектам интеграции (речь идет о рабочих процессах на основе событий или с отслеживанием состояния) распределенных приложений, которые напрямую взаимодействуют с потоками управления приложениями и бизнес-логикой. То, что я здесь называю «Облаком приложений», это совокупность облачных сервисов, имеющих отдельные API-интерфейсы и взаимодействующих с приложением через специально созданные конечные точки.

Инфраструктура, ориентированная на приложения

В этой только что начавшейся облачной эволюции облачные сервисы «сырой» инфраструктуры (такие как AWS EC2) отодвигаются на задний план и становятся прозрачными для разработчиков. Возникает новое облако бессерверной инфраструктуры, такое как AWS App Runner, которое работает на уровне детализации приложения, а не виртуальной машины, отвечает за выполнение приложения, масштабирование, конфигурацию и сетевое взаимодействие. Облачная инфраструктура трансформируется в ориентированную на приложения бессерверную среду выполнения и сетевого взаимодействия.

Более интересный аспект этой эпохи — появление облачных сервисов, которые сочетаются с потоками управления приложениями. Это службы интеграции для организации рабочего процесса, управляемого событиями. Эти службы отслеживают состояния и взаимодействуют с приложением непосредственно через конечные точки приложения. Такие облачные сервисы могут быть явно подготовлены и сконфигурированы или динамически созданы по запросу из DSL в коде приложения. В качестве примера можно привести пошаговые функции AWS, рабочие процессы Google Cloud или рабочие процессы Temporal Cloud, которые организуют последовательность операций, выполняемых в вашем приложении. Или AWS Event Bridge, который доставляет отфильтрованные и преобразованные события в ваше приложение, или EventArc от Google. Или бессерверная служба Dapr, которая связывает сторонние API, триггеры на основе Cron и другие приложения с вашим. Эти новые службы «Облака приложений» связаны с приложением на более глубоком уровне, чем бессерверная служба среды выполнения, отвечающая только за жизненный цикл приложения.

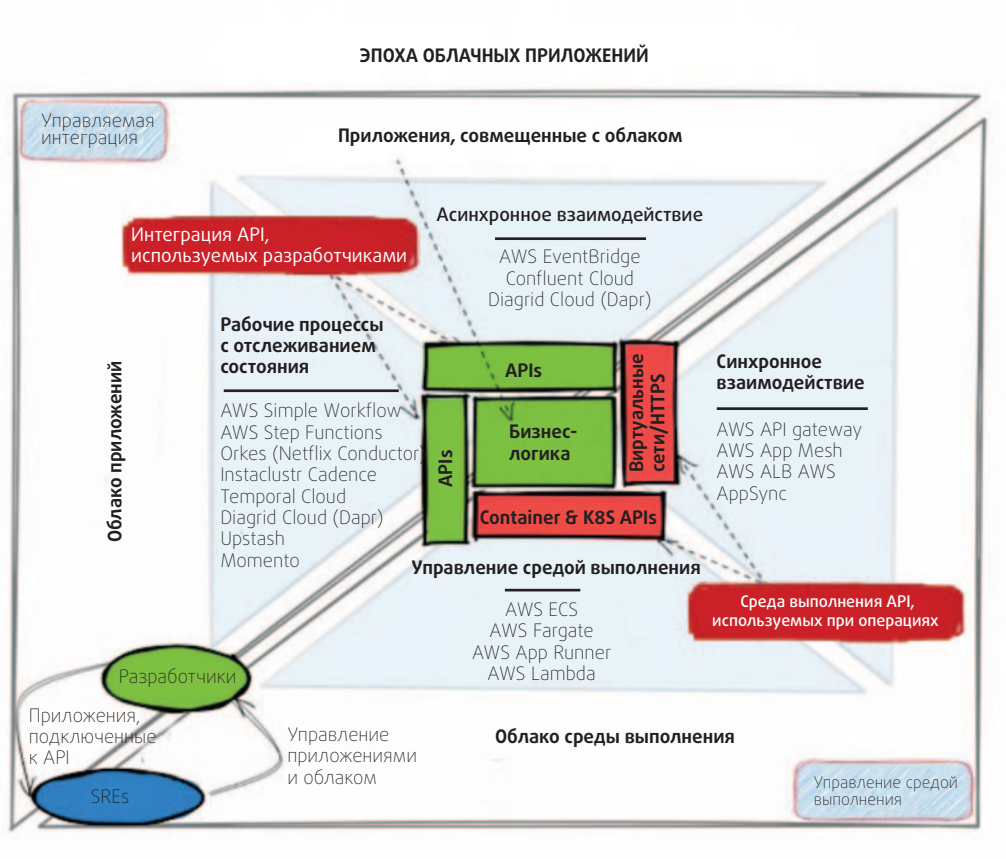


Рис. 4. Приложения в сочетании с облачными сервисами среды выполнения и интеграции.

Облачные приложения

В данной модели код приложения, будь то микросервисы или функции, подключается к облаку во время выполнения программы и сливается с ним. В такой архитектуре часть потока управления приложением выполняется внутри кода приложения, а часть — в облачных сервисах.

«Облако приложений» не определяет, основано ли ваше приложение на микросервисах, функциях или чем-то еще. В этой модели часть логики интеграции и управления приложениями выгружается в облако и используется как услуга. Это форма использования сложных и повторяющихся

специализированных конструкций разработчика посредством четких API-интерфейсов и гарантированных соглашений об уровне обслуживания, а не их реализация или импорт в приложение. Эти конструкции могут быть службой соединения, вызывающей метод приложения, службой оркестровки с отслеживанием состояния, которые вызывают конечные точки приложения для фиксации бизнес-транзакции или точку выхода в случае сбоя. Это может быть просто конечная точка распределенной блокировки, триггер на основе Cron или уведомление об обновлении конфигурации. Используя эти примитивы в качестве бессерверной службы, разработчики приложений могут сосредоточиться на реализации уникальной бизнес-логики, а операционные группы — на управлении и контроле лучших в своем классе реализаций служб.

Открытый исходный код как источник де-факто API

Чтобы «Облако приложений» могло связываться с приложением таким образом, чтобы его можно было заменить другими сервисами, ему необходим четкий API, который может вызываться приложением или наоборот. В идеале этот API должен быть общепринятым, многоязычным и независящим от облака, точно так же, как контейнеры и Kubernetes абстрагируют инфраструктуру и сеть. Такие API-интерфейсы должны получить широкое распространение и стать стандартом де-факто в своих областях, точно так же как контейнеры используются для упаковки и изоляции ресурсов, а Kubernetes — для их оркестровки. Сегодня одним из проверенных способов создания таких стандартов API де-факто является использование модели разработки с открытым исходным кодом в сочетании с прозрачной моделью управления нейтральной программной основой. Удачными примерами этих API являются такие проекты, как Open Tracing, Prometheus для метрик, Kafka для журналов событий, Dapr для интеграции и т.д. Есть также примеры отраслевых стандартов, которые возникли не из среды открытого исходного кода и открытого управления, например, GraphQL для запроса данных, AWS S3 для хранилища объектов и другие. Все это примеры стандартов API, которые фактически используются в приложениях и в конечном итоге становятся доступными в виде облачных сервисов сами по себе.

Краткий итог

В этой статье мы рассмотрели несколько тенденций, которые происходили и одновременно усиливали друг друга. Инфраструктура переехала из локальной среды в облако. Архитектура приложений, находящаяся на вершине пирамиды, перешла от монолитной архитектуры к микросервисам и функциям. Пока происходили эти изменения, контейнеры и Kubernetes представили абстракции жизненного цикла, специфичные для приложений, и сместили фокус инфраструктуры на уровень приложений.

В условиях, когда все крупные облачные провайдеры переключают внимание на среду выполнения, ориентированную на приложения и сервисы интеграции, самый масштабный переход еще впереди. Увеличивается число облачных сервисов приложений для организации событий и управления состоянием. Это новое поколение сервисов, которые объединяются с приложением для предоставления надежно защищенного способа разработки. Эти прикладные сервисы изменят взгляд на архитектуру приложений, превратив ее из единого модуля развертывания в единое целое с облаком. Создание нового поколения облачных сервисов, образующих новое «Облако приложений», только началось.

Литература:

https://www.diagrid.io/blog/evolution-of-cloud-computing

Об авторе:

Билгин Ибрям (Bilgin Ibryam), руководитель продукта в Diagrid, работающий над API-интерфейсами для повышения производительности разработчиков,
https://www.diagrid.io/contact-us

Приложения, сочетающиеся с облачными сервисами среды выполнения и интеграции

	Дооблачная эпоха (2000)	Эпоха облачной инфраструктуры (2010 г.)	Эпоха облачных приложений (2020 г.)
Архитектура приложения	Монолит (например: SOA/ESB)	Микросервисы, функции	Микросервисы и функции, связанные с облаком
Интеграция	Обмен сообщениями и рабочие процессы **[управляются разработчиками]**	Контейнеризованное промежуточное программное обеспечение **[управляется операторами]**	Новое «облако приложений» **[управляется облаком]**
Среда выполнения	Жизненный цикл и сеть **[управляются разработчиками]**	Kubernetes и сервисная сетка **[управляется операторами или облаком]**	«Облако среды выполнения» в первую очередь для приложений **[управляется облаком]**
Поддерживающая инфраструктура	Локальная **[управляется операторами]**	Облачная **[управляется облаком]**	Скрытая **[управляется облаком]**

Децентрализация облаков в общем тренде развития IT-индустрии

Марат Биктимиров

Облачные вычисления сегодня являются основой цифрового бизнеса. В последнее десятилетие эта отрасль развивалась необычайными темпами. Растущий интерес к облачным вычислениям вызывает ускорение технологических преобразований, в результате которых появляются тысячи новых облачных функций.

Такой темп инноваций в целом полезен, но, с другой стороны, приводит к усложнению действующей IT-инфраструктуры, а риски, связанные с облачными вычислениями, существенно возрастают. Поскольку системы облачных вычислений сугубо централизованы, любые перебои в предоставлении облачных услуг становятся крайне нежелательным явлением. По данным Cloud Academy [1], время простоя часто называют одним из самых больших недостатков облачных технологий.

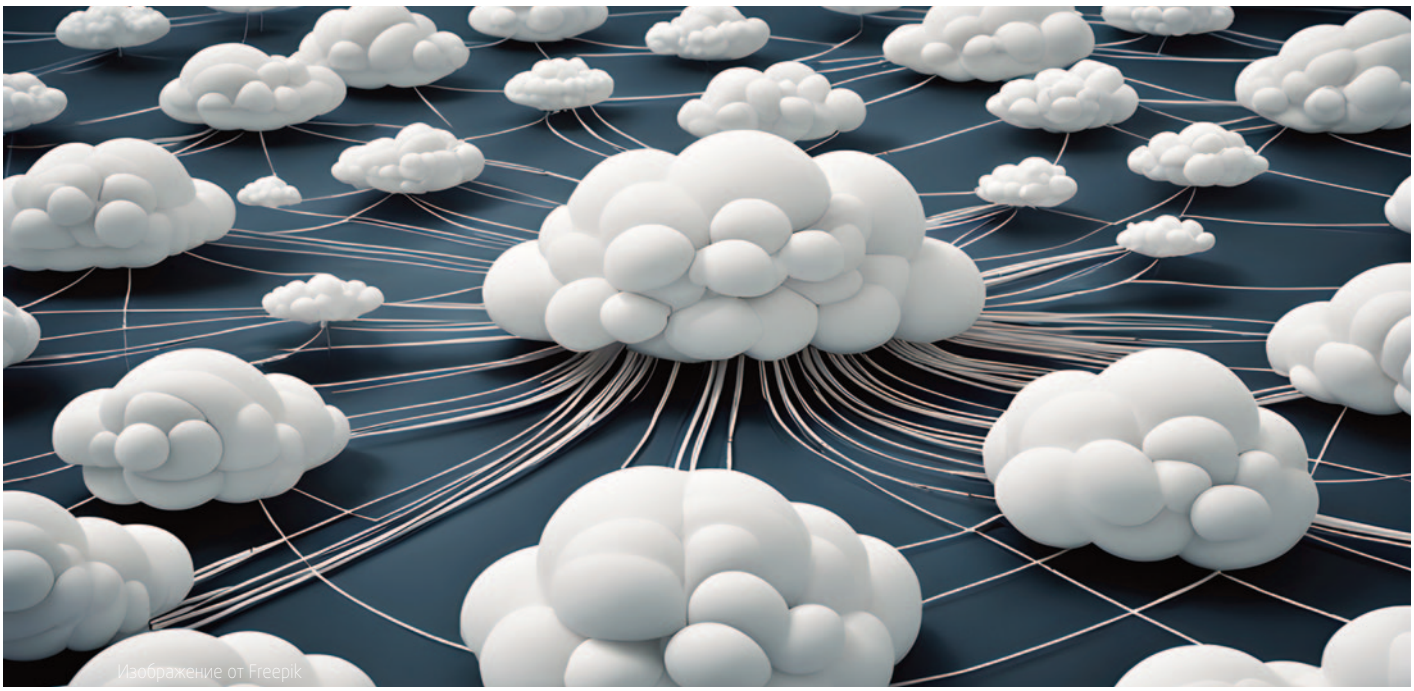
Многие теперь задаются вопросом: как централизованная облачная инфраструктура может поддерживать взрывной рост данных и вычислительной мощности, гарантируя при этом устойчивость, безопасность, масштабируемость и оптимизацию ресурсов одновременно? Сегодня организации по всему миру осознали, что для удовлетворения требований к современной цифровой бизнес-инфраструктуре требуется искать децентрализованные подходы.

То, что новой тенденцией в мире информационных технологий стала децентрализация, – свершившийся факт. Многие проекты уже сегодня пробуют перевести свои сервисы с клиент-серверной архитектуры на формат взаимодействия «клиент-клиент». Одним из определений децентрализации считается отсутствие единого центра контроля и единой точки отказа. Для чего это вдруг стало нужно, в чём причина такой метаморфозы и причём тут «облака»? Попробуем разобраться.

Мир перешел в онлайн и всё, что мы делаем сегодня в Интернете, все веб-приложения и социальные сети, – всё стало жить в центрах обработки данных (ЦОД).

Для того, чтобы предлагать услуги онлайн, бизнесу требуются скоростные каналы связи и мощные вычислительные ресурсы, предназначенные для обработки больших массивов данных. Это достаточно дорогое удовольствие, которое потенциально содержит риск ошибочной оценки, неверно спрогнозировавшей текущую и перспективную технологическую потребность [2].

Сегодня проблема владения вычислительными средствами эффективно решается с помощью услуг ЦОД – центров коллективного пользования, предоставляющих своим клиентам в аренду серверные мощности и обеспечивающих к ним высокоскоростной доступ. Такие ЦОД, как правило, управляются одной компанией — провайдером услуг, и вместо покупки собственного оборудования клиент арендует у провайдера масштабируемую в зависимости от текущих потребностей вычислительную мощность и пространство для хранения данных.



По мере развития этих услуг перестало быть важным, на каком конкретном сервере или даже в каком ЦОД находятся и обрабатываются те или иные данные. Теперь это называется просто «облако» – нечто расплывчатое, но всеохватывающее. Облачные провайдеры услуг конкурируют друг с другом по цене за вычислительную мощность, хранилище и трафик. При этом облачная инфраструктура предоставляется пользователю в качестве технологической страты, о принадлежности которой он обычно вспоминает, только когда сломается его веб-сайт или служба.

Сегодня практически каждый сервис, работающий онлайн, мигрировал в облако. Это, с одной стороны, приводит к существенному повышению производительности, но с другой – создает новые риски, а также новые требования к информационной защите, поскольку в этих сервисах циркулируют критически важные и приватные данные. Ну и традиционная задача выделения достаточного количества серверов для корректной работы не только никуда не делась, но и остается постоянной головной болью даже для крупных облачных провайдеров.

Итак, чтобы перевести весь мир в онлайн, пришлось изобрести совершенно новый системообразующий элемент IT-

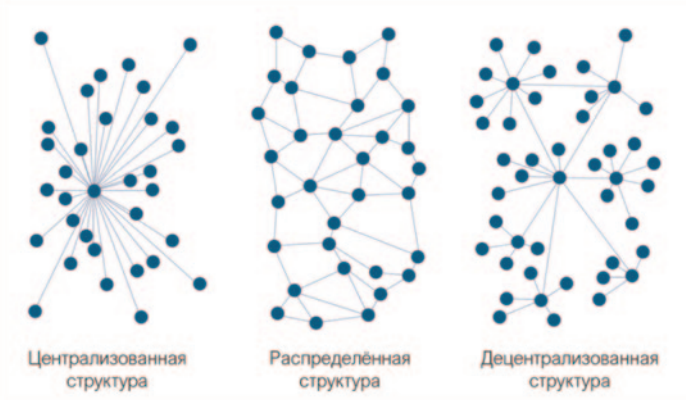


Рис. 1. Типология структур.
Источник: www.cleanpng.com

инфраструктуры: ЦОД. Однако, как говорится, «недолго музыка играла», и очень похоже, что мы стоим на пороге новых инфраструктурных преобразований.

Рис. 2. Облако сервисов.
Источник: libertyadvisorgroup.com

В современном центре обработки данных могут одновременно работать десятки тысяч серверов. Они работают 24 часа в сутки 7 дней в неделю и требуют постоянного ухода и обслуживания. Иными словами, то, что делают эти ЦОД – не что иное, как управление информационной инфраструктурой, которую назвали «облаком». Облачные сервисы растут с необычайной скоростью. Объем данных в сферах связи и телекоммуникаций, бизнеса и финтеха, игровых и бытовых приложений, а теперь и в области искусственного интеллекта приближается к десяткам и даже сотням зетабайт. Масштабы требуемой под эту лавину инфраструктуры сложно себе представить. Как следствие – «облака» стали в полном смысле критически важной инфраструктурой. Поэтому и поиск решений для улучшения надёжности и

управляемости этой инфраструктуры предвосхищает новые, по сути своей революционные изменения.

Сегодня ЦОД потребляют колоссальное количество электроэнергии. По некоторым оценкам, на них приходится около двух процентов всего мирового энергопотребления. При этом большая её часть используется для охлаждения серверного и обеспечивающего оборудования. В связи с этим ЦОД стало выгоднее располагать в регионах с более дешёвым электричеством и умеренным климатом. Кроме того, появляется всё больше запросов на оптимизированное с точки зрения загрузки серверных мощностей программное обеспечение. Возможно, при нынешнем росте объёмов вычислительных операций это тоже сможет оказать определённое влияние на энергоёмкость ЦОД. Однако как оптимизировать растущее энергопотребление?

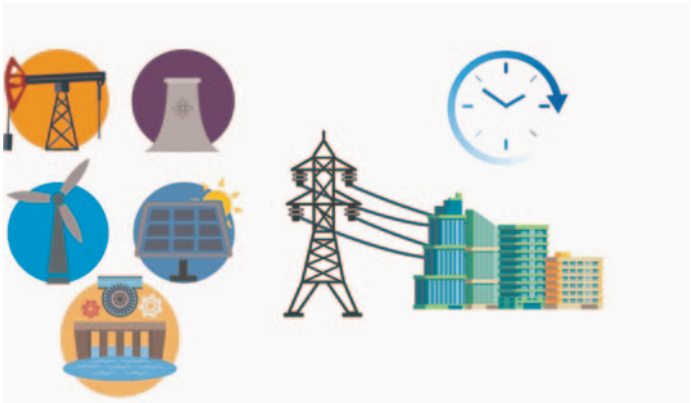


Рис. 3. Энергопотребление ЦОД.
Источник: www.datacenterknowledge.com/

Ещё одна не менее существенная проблема, как ни парадоксально, заключается в неэффективном использовании ЦОД. На поверку оказывается, что реально клиенты используют только часть серверных мощностей. Объясняется это, прежде всего, циклическим изменением объёма потребляемых услуг в зависимости от времени суток в пределах одного часового пояса. К примеру, ночью обычно заняты лишь единицы процентов ресурсов ЦОД – при том, что весь остальной ЦОД работает «вхолостую», продолжая потреблять энергию и выделять тепло. Оценочно в среднем используется только 15% мощности. Какая уж тут эффективность, когда 85% ЦОД просто греют атмосферу?!

Казалось бы, решение напрашивается само собой: находить и максимально использовать недозагруженные серверы, а не запускать всякий раз новые под каждую новую задачу. Логично предположить, что для любого перегруженного в определённый период времени ЦОД где-нибудь найдётся недогруженный или более того – малоиспользуемый ЦОД, на серверы которого можно было бы перенаправить избыточную вычислительную потребность.

Конечно, при этом неизбежно возникает напряжённость в сетях передачи данных, а для некоторых приложений качество связи весьма и весьма критично. Тем не менее, можно допустить, что для большой части задач такая альтернатива окажется вполне рабочей.

Очевидно, что здесь необходима оптимальная и широкомасштабная системная организация процесса. И тут мы переходим к идее децентрализованных облачных вычислений: вспомним, например, незаслуженно отодвинутую на периферию современных трендов идею распределённых вычислений под названием грид.

Концепция грид-вычислений возникла четверть века тому назад для проведения сложных расчётов в больших научных задачах. Для решения были необходимы такие объёмы ресурсов, которые бы значительно превосходили мощности локальных компьютерных систем, имевшихся в отдельных исследовательских организациях или научных центрах коллективного пользования.

Грид предложил новый подход, позволяющий решать большие задачи на существующей аппаратной базе. Суть подхода состояла в том, что расчётные задачи могут выполняться на совокупности ресурсов некоторого множества вычислительных систем. Такая концепция определяла принцип образования грид-инфраструктуры из распределенных в глобальном сетевом пространстве ресурсов и обеспечения к ним удаленного доступа из компьютерных приложений. Интеграция вычислительных ресурсов в грид-инфраструктуру, естественно, не ставила задачей изменение состава этих ресурсов, но задавала условия, при которых любая часть или даже все они могли бы использоваться для решения одной или нескольких больших задач.

Фактически, в качестве ресурсов рассматривались любые элементы, участвующие в вычислительном процессе: от «железа» до «софта». Соответственно, доступ к ним предусматривал дистанционный запуск и управление программными средствами на удалённых вычислительных машинах, а также размещение файлов в распределенных системах хранения.

Таким образом, грид рассматривался как виртуальный суперкомпьютер, объединяющий распределённые вычислительные машины посредством какой-либо шины, например, Ethernet или даже Интернет.

Но ведь и облако использует Интернет. В чём отличие? Целью облачного компьютинга, равно как и у грид, является интеграция большого количества ресурсов и обеспечение

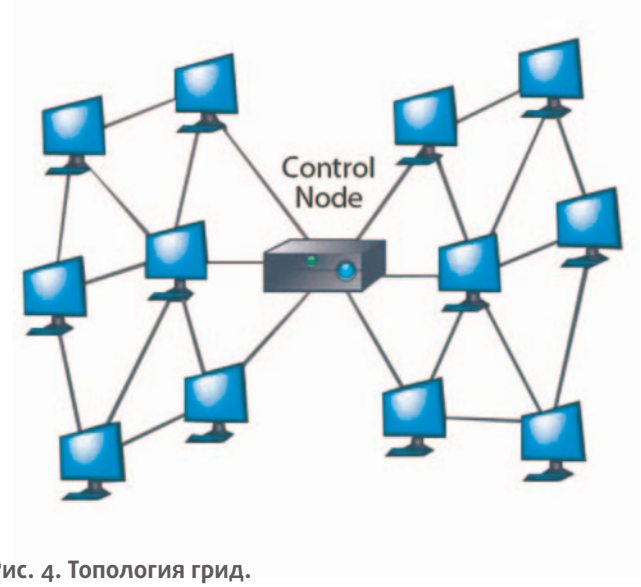


Рис. 4. Топология грид.
Источник: вебджем.рф

к ним удаленного доступа. Однако оба они используют разные способы организации и использования этих ресурсов.

В основе грид лежит распределённый подход: инфраструктура создаётся путём программной интеграции автономных ресурсных узлов с собственными системами управления с помощью так называемого MiddleWare (промежуточного или связующего программного обеспечения).

А облачные вычисления используют одноуровневую организацию инфраструктуры в виде облака. Все ресурсы облака управляются централизованной системой, которая, в частности, обеспечивает к ним прямой удалённый доступ [3].

И если сейчас облака в основном развиваются по пути расширения до огромных «облачных фронтов», то несложно предположить и правомерность другого способа развития вычислительной инфраструктуры: посредством интеграции различных облаков по технологии грид. Тогда средствами облачной технологии осуществляется управление ресурсами конкретного облака, а грид отвечает за поддержку вычислительных процессов в глобально распределённой среде, которая объединяет облака провайдеров. Тут необходимо сказать, что прообраз облачного грида был создан ещё в 2014 году в рамках европейской научной грид-инфраструктуры. Здесь в основу интеграции был положен принцип непосредственного доступа ко всему множеству ресурсов, содержащихся в инфраструктуре облаков в соответствии с моделью обслуживания IaaS [4].

А что же нынешний бизнес с его модной приверженностью к облачным платформенным решениям PaaS? Очевидно, при таком подходе должна появиться возможность объединения облаков разного размера и разной локализации и, как следствие, возможность оптимального распределения нагрузки на ресурсы между ними в рамках одного платформенного решения. Децентрализация? В каком-то смысле, да, но...

В настоящее время бизнес-модель крупных поставщиков публичных облачных сервисов предполагает продвижение исключительно своих собственных платформенных решений как универсальных и охватывающих буквально все требования потенциального клиента, препятствуя претензиям конкурентов на «завоёванные территории».

Рис. 5. Блокчейн.
Источник: www.analyticsinsight.net

В то же время на практике всё чаще возникает потребительский запрос на гибридные или мультиоблачные среды. А это означает, что провайдеры должны обеспечить интероперабельность между своими платформами. Возникает противоречие между интересами крупного провайдера, желающего продавать как можно больше облачной ёмкости растущему потребителю, и интересами клиента, который стремится эффективнее использовать возможность работы одновременно в нескольких облаках, например, когда нужно обмениваться данными с партнёрами, работающими с различными стандартами данных и бизнес-приложениями.

Вопрос в том, как сделать это глобально и надежно? Как вывести на общий облачный рынок провайдеров разного калибра?

Например, это можно сделать, объединив облачных провайдеров в некий консорциум, в котором они договариваются продавать свои ресурсы в соответствии с установленными правилами, не отвергающими ценовую конкуренцию. Для этого потребуется сформировать единую платформу, на которой провайдеры на равных смогут предлагать свои возможности клиентам.

Такая полностью автоматизированная платформа должна стать открытой, прозрачной и надёжной, чтобы поставщики и клиенты могли с уверенностью покупать и продавать облачные ресурсы. Она может функционировать на принципах так называемого обратного аукциона, когда несколько участников-членов консорциума предлагают аналогичные услуги и конкурируют друг с другом за одного клиента, который сможет выбирать между их предложениями. Это работает только в том случае, если есть уверенность, что все участники аукциона добросовестны.

Тут самое время вспомнить о блокчейне. Как известно, термин «блокчейн» объединяет в себе разные развивающиеся технологии с одной и той же архитектурой: общий неизменный онлайн-реестр, позволяющий безопасно и публично обмениваться данными и их хранить. В таком случае каждый облачный ресурс можно рассматривать как ноду (от англ. node – узел) сети блокчейна. Гарантом сделки будет выступать не централизованный облачный гигант, способный влиять на рынок, а смарт-контракты, оплачиваемые соответствующими токенами.

Токен являет собой запись в блокчейне, посредством которой каждый поставщик услуг на платформе сможет уверенно представить свои доступные ресурсы и условия для других заинтересованных сторон. Скажем, объём услуги может быть очерчен определенным типом и количеством токенов, которые чётко отслеживаются платформой. Всегда будет достоверно известно, когда, где и сколько ресурсов доступно. Механизм обратного аукциона устанавливает цену, и ни у кого нет никаких возможностей для манипуляций, поскольку все записано в реестре и доступно каждому для просмотра [5].

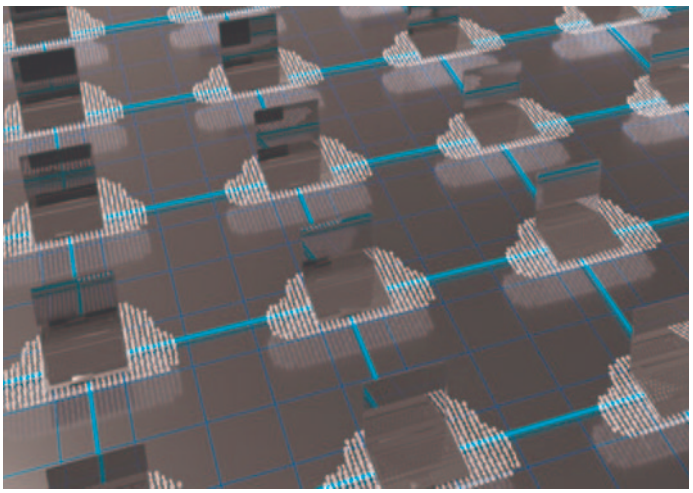


Рис. 6. Грид из облаков.
Источник: stock.adobe.com

В результате, даже платформа, объединяющая небольших провайдеров, гипотетически сможет конкурировать с облачными «гигантами», предоставляя клиентам сопоставимые по качеству и надежности услуги с прозрачной, благодаря использованию блокчейна, ценовой политикой.

Справедливости ради надо сказать, что для многих пользователей выбор между локальным облаком и мультиоблачной децентрализованной средой может стать весьма непростым. И там, и там существуют свои преимущества и недостатки с точки зрения адаптивности, производительности, безопасности и соответствия техническим требованиям.

Представим себе, что в децентрализованных облаках может работать любое оборудование, размещённое в любом месте, куда подведено электричество и Интернет. Это открывает для потенциального пользователя невероятные возможности по конфигурированию арендуемых им мощностей. При этом, опять же благодаря технологии блокчейн, его доступ к вычислениям ограничить практически невозможно.

Соответственно, и стоимость услуги может оказаться значительно ниже, чем у централизованного облачного провайдера.

Но на самом деле не всё так радужно. Облачный провайдер обладает гарантированно надёжной инфраструктурой, обеспечивающей бесперебойный процесс вычислений, а вот нода децентрализованной среды этим похвастаться, увы, не сможет в силу распределённой же ответственности.

Критически важные клиентские данные и алгоритмы потенциально могут быть скомпрометированы излишне любопытным владельцем ноды. Безусловно, в такой ситуации к серьёзному провайдеру доверия будет многократно больше.

При всей привлекательности децентрализованные облачные решения на основе блокчейна представляют собой множество других проблем, таких как:

- обеспечение стимулирования и справедливого распределения доходов между поставщиками ресурсов;
- обеспечение масштабируемости инфраструктуры с учетом ограничений масштабируемости самого блокчейна;
- контроль правильности вычислений во избежание потенциальных вредоносных атак;
- обеспечение оптимального баланса между весом репутации поставщика и стоимостью его выхода на рынок;
- управление правом на удаление данных в случае вредоносной атаки или других сбоев [6].

Поэтому сегодня растёт интерес к тем гибридным или мультиоблачным платформам, в которых, например, потребитель может выбирать только отдельные услуги, отвечающие его запросам. А облачный провайдер волей-неволей вынужден пересматривать свои бизнес-модели предоставления услуг.

В связи с нерешёнными проблемами и слишком очевидными рисками сегодня децентрализованные облака не пользуются особым спросом у потребителей, предложений этой услуги на рынке тоже немного. Тем не менее, распределённые облачные вычисления, безусловно, имеют право на существование и наверняка смогут найти своих потребителей. Ведь платформы децентрализованного использования вычислительных ресурсов на основе блокчейна исследовательские коллективы развивают уже несколько лет [7].

Так, проект ANKR [8] представляет собой децентрализованное облачное решение, ставящее своей целью предложить клиентам инфраструктуру для запуска приложений по более низким ценам по сравнению с ценами традиционных поставщиков облачных услуг, а ЦОД – инфраструктуру для создания новых источников дохода за счет их недостаточно используемых вычислительных мощностей. Это должно быть достигнуто за счет обеспечения высокого уровня доступности услуг, простой интеграции и безопасной связи.

А проект Dfinity [9] представляет собой децентрализованное облачное решение, целью которого является предоставление условному мировому суперкомпьютеру «бесконечной» вычислительной мощности. Здесь применяется концепция «Искусственный интеллект – это закон», в которой всё подчиняется алгоритмической системе управления без посредников, сочетающей в себе «мудрость толпы» и традиционные технологии искусственного интеллекта для замораживания вредоносных смарт-контрактов, которые могут нанести ущерб интересам тех, кто использует платформу. Это фактически означает, что некоторые транзакции могут быть изменены и возвращены обратно, если они не одобрены системой алгоритмического управления, что является противоположным подходом по сравнению с такими криптовалютными проектами, как Bitcoin или Ethereum, где действует правило «Код – это закон», по которому пользователь фактически не может вернуть транзакцию после обработки.

К сожалению, децентрализованные облачные архитектуры на основе блокчейна все еще находятся в зачаточном состоянии, и по этой причине такие важные показатели, как качество обслуживания, производительность, масштаби-

Рис. 7. Децентрализованные облачные вычисления.
Источник: stock.adobe.com

руемость, безопасность этих платформ будут иметь решающее значение в соперничестве с классическими облачными инфраструктурами.

Однако не будем забывать, что собственно Интернет изначально был задуман как децентрализованная система, хоть и развивался под воздействием мощных центростремительных сил. Стремление к росту прибыли, увы, почти всегда приводит к централизации. Но практика показывает, что в конечном счёте централизованные системы проигрывают. Во-первых, они не безразмерны, а во-вторых, плохо сочетаются с процессами трансформации современного мироустройства. Жизнь становится все более сложной, и централизованные системы не выдерживают свалившейся на них нагрузки.

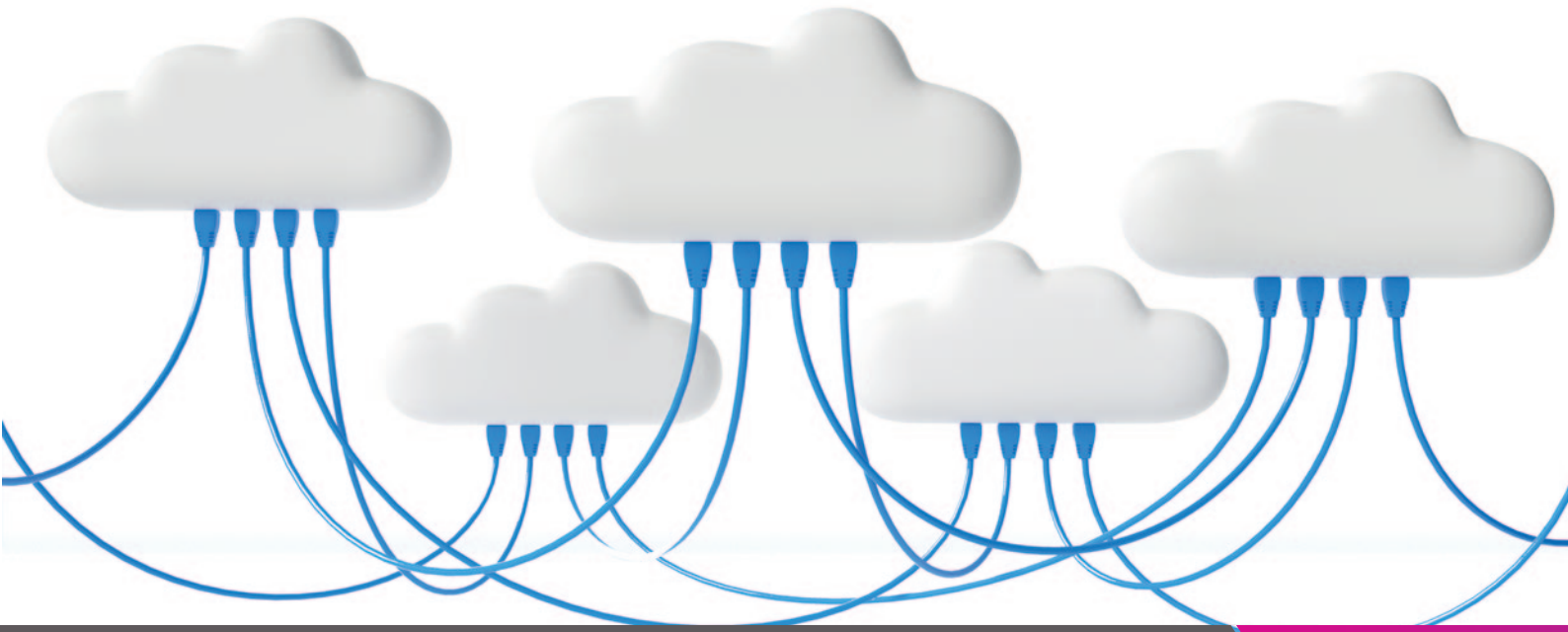
Наша цивилизация богата ресурсами и неравнодушными людьми, ищущими способы их рационально использовать. Есть стойкое ощущение, что облака вкупе с блокчейном тоже поучаствуют в преобразовании реальности, требующей нового осмысления, и создадут, наконец, в отрасли «атмосферное» явление следующего поколения.

Литература

[1] Cloud Academy, «Disadvantages of Cloud Computing», June 2018. [Online]. Available: https://cloudacademy.com/blog/disadvantages-of-cloud-computing/
[2] Kelsey Ruiz, «Architecture Series Part I: The Cloud», November 2021. [Online] Available: https://akash.network/blog/architecture-series-part-i-the-cloud/
[3] Схандип Бхандари, «Грид-вычисления против облачных вычислений: разница и сравнение» URL:https://askanydifference.com/ru/difference-between-grid-computing-and-cloud-computing/
[4] Коваленко В.Н., Коваленко Е.И. Новый этап развития грида: грид из облаков // Препринты ИПМ им. М.В.Келдыша. 2018. No 168. 22 с. doi:10.20948/prepr-2018-168 URL: http://library.keldysh.ru/preprint.asp?id=2018-168
[5] @drakononov, «Децентрализованные облачные вычисления — благо или зло?», URL: https://habr.com/ru/articles/709100/
[6] R. Brundo Uriarte and R. De Nicola, "Blockchain-Based Decentralised Cloud/Fog Solutions: Challenges, Opportunities and Standards," September 2018. [Online]. Available: https://www.researchgate.net/publication/326346449_Blockchain-Based_Decentralised_CloudFog_Solutions_Challenges_Opportunities_and_Standards
[7] Mattia Mrvosevic, «Blockchain Based Decentralised Cloud Computing», Eterna Capital, February 2019. [Online] Available: https://eternacapital.medium.com/blockchain-based-decentralised-cloud-computing-277f307611e1
[8] C. Song, S. Wu, S. Liu, R. Fang and Q.-L. Li, "ANKR — Build a Faster, Cheaper, Securer cloud using idle processing power in data centers and edge devices," [Online]. Available: https://www.ankr.network/
[9] T. Hanke, M. Movahedi and D. Williams, "Dfinity — The Internet Computer," [Online]. Available: https://dfinity.org/faq/

Об авторе:

Марат Рамилевич Биктимиров, руководитель научно-образовательных проектов Фонда развития сетевых технологий «ИнДата».



Протоколы в туннелях и будущее Сети на примере DoH и ECH

Александр Венедюхин

Почти десять лет назад появились первые предложения о DNS-over-HTTPS (DoH). Тогда некоторые восприняли идею как шутку и даже выдвигали иронические варианты развития, например, DNS-over-GIF и другие занимательные версии. Однако в 2016 году поддержку DoH добавили на сервис DNS-резолвинга Google Public DNS, а несколько лет спустя DoH стал чем-то вроде стандартного инструмента для работы с DNS, как с сервисом, в веб-браузерах, после чего иронизировать на тему данной технологии стало дурным тоном.

DNS-over-HTTPS — хороший пример того, как изменение технологического ландшафта Интернета приводит к перемешиванию ранее привычных уровневых структур (типа устаревшей модели OSI из семи уровней): старые протоколы, чтобы продолжать работать в новых условиях, пробивают в изменившемся ландшафте туннели.

DoH представляет собой удобный программный интерфейс (API) к совсем другому сервису, а не к DNS как к системе – то есть это надстройка через два новых уровня абстракции. При этом в описаниях DoH нередко можно прочитать, что данная технология позволяет отказаться от сложностей DNS. Сколь бы странным это ни казалось, но спорить тут не о чем: если прикладная программа использует тот или иной сервис, предоставляющий DoH, то эта программа работает уже только с HTTPS и данные получает по этому же протоколу, в весьма удобном формате JSON – и действительно, в этом случае взаимодействие с DNS для прикладной программы исчезает. Другое дело, что из типичного системного окружения узла, подключенного к Интернету, на котором эта прикладная программа работает, DNS никуда не девается: даже для инициализации DoH-сервиса всё равно нужно непосредственно использовать классический доступ к системе доменных имён. Это несмотря на возможность настроить непосредственно сам IP-адрес (известные примеры: 8.8.8.8, 1.1.1.1). То есть классический доступ к DNS через «обычный» локальный резолвер никуда из системного окружения не исчезает.

Перенести решение задач DNS на другой фундамент, включающий и TLS, и HTTP, предлагается дополнительно. Конечно, базовый протокол DNS имеет свои особенности и большое количество «крайних случаев», но сложность сочетания TLS с HTTP на порядок выше. Можно предположить, что в случае браузера поддержка и интенсивное использование TLS и HTTPS так или иначе необходимы, поэтому перенос на эту базу ещё и API доступа к DNS (то есть реализация DoH) ничего не меняет. Но, во-первых, схема тут работает в обе стороны: перенос ещё одной базовой технологии в уже имеющийся стек означает, что уязвимости и риски этого стека начали работать и для вновь поступившей технологии – в данном случае, возможные проблемы с TLS повлияют и на доступ к DNS. Во-вторых, как говорилось ранее, DNS никуда не девается из системного окружения.

Тогда почему же DoH? Базовая причина в том, что самая современная модель управления доверием в задачах информационной безопасности предполагает доверие именно между приложениями, а DoH как раз и позволяет изолировать доступ к важнейшему сервису от системного окружения, в котором конкретное приложение исполняется. Приложение «веб-браузер» с настроенным сервисом DoH создаёт туннель прямо из своего контекста до приложения «поиск в DNS» на удалённом DNS-сервисе. В рамках штатной работы приложения туннель закрыт не только для других приложений, но даже и для ядра ОС (естественно, с оговорками о том, что на уровне ядра ОС получить доступ к данным приложения внутри TLS труда не составляет). Несомненно, использовать DoH можно и для доступа к «локальному» резолверу провайдера, но это не отменяет необходимости поддерживать и «классический» вариант доступа к провайдерскому резолверу, потому что со стороны клиента DoH есть только в избранных приложениях. То есть туннели DoH здесь прямо влияют на сетевую реальность, усложняя её.

Классический вариант доступа к DNS предполагает использование протокола UDP в качестве сетевого транспорта и запросы/ответы в пакетах DNS-формата. DoH же переводит логику доставки на два уровня выше, заменяя UDP на TCP и добавляя TLS, а поверх него – HTTP, при этом запросы/ответы упаковываются в новые структуры (JSON), которых не было в DNS, а для установления TCP-соединения всё равно может потребоваться доступ к DNS.

В «классическом» Интернете сетевому инженеру нужно было бы настроить DNS-сервер (резолвер) с доступом для конечных клиентов и проверить, что DNS-пакеты успешно доставляются в обе стороны. При этом в более продвинутых вариантах в резолвере могут быть настроены разные зоны и применяться различные методы обработки запросов и имён для отдельных клиентов. Предположим, что теперь нужно перейти к использованию DoH. Дополнительно потребуется настроить TLS/HTTPS. И даже если сервер резолвинга с DoH «локальный» и для него используется программное обеспечение резолвера, в котором DoH доступен из коробки, придется настроить пропуск дополнительного типа трафика (TLS) к DNS-серверу.

Если же клиентом подключается внешний DNS-сервис с DoH, например, Cloudflare или Google, то на стороне провайдера доступа полностью утрачивается возможность локальных настроек зон и правил обработки имён. Для кого-то из пользователей это хорошо, а для кого-то – не очень: так, когда что-то не работает, не слишком продвинутые пользователи внешних сервисов DNS могут стать проблемой для службы поддержки, которой приходится догадываться, что на самом деле имеет в виду пользователь. При этом продвинутые пользователи могут получить защищённый канал до резолвера. Но в любом случае на примере DoH видно, что сдвиг парадигмы в сторону «доверия между приложениями» на сетевом уровне проявляется в виде «спагеттизации» протоколов: то, что раньше успешно ходило на своём «плоском» уровне через UDP, вдруг обрело дополнительное измерение и выписывает кривые между плоскостями. И хоть в DoH есть туннель, но это ещё не VPN.

Раньше считалось, что протоколы и сервисы работают на своих уровнях. Например, до начала HTTP-сессии сначала задействовалась DNS через UDP, а дальше, после обнаружения нужного IP-адреса и установления TCP-соединения, HTTP-клиент мог отправить команду на HTTP-сервер. Современное направление развития протоколов таково, что логические концепции размазываются и самокопируются между уровнями и туннелями: HTTP/2 затягивает в себя концепции из слоя TCP (например, разделение обмена данными на асинхронные потоки, которые, тем не менее, организованы внутри одного соединения, повторную передачу сообщений и т.д.), при этом TCP либо никуда не исчезает, либо заменяется на UDP (см. QUIC — Quick UDP Internet Connections, транспортный протокол, изначально разработанный Google и стандартизованный в IETF), но с ещё более широкими надстройками, логически копирующими аспекты TCP по управлению сессией. С одной стороны, это даёт заметные преимущества, но с другой стороны, приносит новые, неожиданные направления атак, основанных именно на переносе логических конструкций между уровнями. На надстройки накладывается практика блокирования доступа, которая едва ли уже не стала всеобъемлющей. Современное состояние этой практики тоже включает несколько логических слоёв: блокирование по «географической привязке адреса», блокирование на стороне веб-сервиса, блокирование на уровне «классической» DNS, блокирование на стороне провайдера доступа, на стороне «облачного» провайдера, на промежуточных узлах (в обе стороны) – список не полный. Всё это сдвигает парадигму: поток сообщений HTTP/2 уже не получается ограничивать на уровне простого файрвола по количеству запросов с одного IP-адреса по номеру порта на сервере.

Типичный сценарий подключения пользователя к веб-сервису состоит (в сетевом смысле) из работы некоторого DNS-резолвера у провайдера доступа и работы NAT этого же провайдера. Однако в реальности ситуация часто оказывается гораздо сложнее: у конечного пользователя теперь настроен VPN, иногда – более одного VPN, каждый из этих VPN выполняет трансляцию адресов (получаем несколько NAT), сервис DNS частично завёрнут в VPN, частично работает через провайдера, а частично – через тот или иной внешний DNS-сервис (см. про DoH выше). Уже достаточно новых измерений для построения непростых сечений многомерных объектов. Однако есть и ещё один важный аспект, набирающий популярность: мы говорим о сервисах скрытого туннелирования.

Хорошим примером такой технологии является ECH (Encrypted Client Hello). Это способ дополнения TLS, позволяющий через тот или иной узел-посредник подключиться к скрытому сервису по TLS, не раскрывая ни имени, ни адреса этого сервиса для стороны, прослушивающей канал.

По сути, ECH с сопутствующими DNS-записями предоставляет универсальный интерфейс для туннелирования. При этом в DNS публикуются открытые ключи и конфигурация доступа. Размещение данных в DNS тут же диктует использование, как минимум, DNSSEC, но скорее DoH (или DNS-over-TLS, DoT), так как сокрытие запросов, связанных с получением конфигурации, увеличивает степень защиты от утечки информации о соединении.

ECH вместе с DoH прекрасно иллюстрируют концептуальные изменения в использовании Интернета и показывают направление расширения технологического базиса. Конечно, подобные схемы применялись и раньше, но это были весьма и весьма специализированные решения для обхода сетевых блокировок с развитым DPI – мало кто их когда-то применял и даже о них слышал (речь про варианты ShadowSocks, модификации XTLS и др.). ECH же – это полноценное развитие TLS со своими RFC, это технология, уже поддерживаемая крупными провайдерами как сервисов доставки контента (Cloudflare [1]), так и клиентского ПО (Mozilla Firefox [2], Google Chrome [3]).

Схема работы ECH следующая [4]. Обычное TLS-соединение начинается с отправки клиентом специального «сообщения-приветствия» – ClientHello. Исторически сложилось, что вокруг этого сообщения и строится ECH. Дело в том, что сообщение ClientHello не только определяет часть параметров соединения, но также обычно содержит в открытом виде имя TLS-узла, к которому собирается подключаться клиент – поле с именем узла называется SNI (Server Name Indication), и промежуточные узлы могут его прочитать. Такая конфигурация тоже сложилась исторически из практики веб-хостинга: указание имени SNI, в частности, требуется для того, чтобы можно было на узле с одним IP-адресом размещать разные виртуальные TLS-узлы. Именно из попыток скрыть имя SNI и выросла технология ECH, а возможность работы разных сервисов на узле с одним IP-адресом тут получает дополнительное развитие: IP-адрес переносится на уровень, совсем не связанный с сервисом, к которому подключается клиент. На начальных этапах проектирования ECH, когда прообраз ещё назывался ESNI, предлагалось относительно простым и прямолинейным способом скрывать только имя, итоговый же результат превратился в интересную, развитую технологию скрытого туннелирования.

В рамках ECH в состав начального сообщения ClientHello верхнего уровня встраивается зашифрованное внутреннее сообщение ClientHello, которое адресовано скрытому проксирующему узлу. Получается, что входной узел организует туннель до скрытого сервиса, который уже обрабатывает внутреннее ClientHello и устанавливает скрытое TLS-соединение с клиентом. Процесс установления соединения полностью соответствует схеме с условным названием TLS-over-TLS. Однако чтобы избежать «двойного» шифрования, последующий обмен данными уже производится между клиентом и скрытым сервисом – входной узел просто копирует данные: то есть клиент обменивается данными через туннель непосредственно со скрытым сервисом.

Таким образом, промежуточный узел, анализирующий трафик, видит только факт установления TLS-соединения (по сообщениям верхнего уровня), которое содержит параметры для, возможно, доступа к скрытому сервису – но этим фактом всё и ограничивается. При этом ECH уже не привязана конкретно к вебу и, например, HTTP. Скрытое TLS-подключение, установленное с использованием ECH, можно использовать для организации полноценного VPN-соединения на более низких транспортных уровнях. Пользователи получили защищённый метод доступа к облачным провайдерам, а с точки зрения сети добавилось несколько туннелей с разными протоколами: по TCP работает TLS-туннель, внутри которого создаётся ещё один TLS-туннель, внутри которого запускается трансляция HTTP-соединения через HTTP-команду Connect.

Массовое внедрение подобных технологий туннелирования, которые не только достаточно сложны сами по себе, но и оптимизируют соединения уже с точки зрения снижения различимости трафика разных типов, приводит к «наложению путей» доставки этого трафика, если процесс рассматривать с точки зрения базовой структуры IP и BGP. Привычный метод описания предполагает, что клиент подключается через несколько промежуточных узлов-маршрутизаторов («ближайших» к нему в сетевом смысле) к оконечным узлам, обеспечивающим работу сервисов, будь то DNS или веб. Однако в реальности при использовании ECH с «универсальным облачным» провайдером, а тем более при использовании VPN, клиентское подключение проходит через те же ближайшие к клиенту узлы-маршрутизаторы, но уже в составе пути к входным узлам в VPN. И лишь дальше, через выходную точку VPN, через совсем другие сетевые пути, клиент подключается к оконечным узлам сервисов.

Для привычных способов использования VPN характерно разделение узлов по IP-сетям: одни сети добавляем в маршруты «через VPN», другие сети – оставляем «без VPN». Но распространение скрытого доступа, подобного ECH, и внедрение DoH вносят новое измерение: направления начинают разделяться по протоколам. Использование разных маршрутов в VPN означает, что к части узлов одного и того же сервиса пользователь-клиент подключается через один набор промежуточных узлов, а к другой части узлов этого же сервиса тот же пользователь-клиент подключается через совсем другой набор промежуточных узлов. Если смотреть со стороны сервиса, то такое подключение будет даже отображаться с другим адресом. Разделение же по протоколам в будущем способно ещё больше усложнить ситуацию.

Такое положение дел, в сетевом смысле, влияет на многие прикладные параметры: «геолокация», балансировка нагрузки и т.д. Неожиданные эффекты возможны с anycast-узлами, особенно – с CDN, где обычным явлением может стать то, что клиент за HTML-разметкой приходит в один дата-центр, а за файлами изображений и трансляцией видео – в совсем другой, да ещё и с разными IP-адресами источника. Не менее странные эффекты происходят со стороны DNS, когда на авторитативные серверы пользователь приходит из одного региона, а на сам сервис, заходя уже через VPN, из совсем другого. Можно было бы этому пользователю выдать для подключения узлы, которые ближе к точке выхода VPN, но сделать это сложнее. Это влияет на эффективные сетевые задержки: например, по одному пути – 30 ms, по другому – 300 ms, и всё это для одного и того же пользователя веб-сервиса в рамках одной сессии.

Расщепление Сети по уровням приложений прямо влияет на процесс статистических измерений в вебе, в том числе и на развитые системы веб-аналитики. Здесь не только теряется большая доля смысла геопривязки пользователя по IP-адресам, но, более того, так как разные элементы одной и той же страницы могут приходить к пользователю через существенно различающиеся между собой сети, показатели сессии размываются. Например, ряд методов измерений в вебе предполагает [5] использование «праймера» — это специальный Javascript-код (JS), исполняемый в браузере. Возможно, что данный JS поступает к пользователю через VPN, но другие измеряемые параметры, связанные с DNS, – уже через «обычное» подключение. С одной стороны, такая ситуация запутывает результаты, но с другой – именно подобное расщепление может послужить инструментом определения степени «перемешивания» уровней подключения на устройстве пользователя, что, теоретически, представляет данные для построения уникального профиля устройства: такой-то VPN и такой-то DNS-сервис – сочетание может быть достаточно редким. Поэтому, хоть в отношении VPN (а также ECH и DoH) регулярно говорят о «приватности», необходимо учитывать, что «разбор» подобных технологий достаточно мощными системами исследования трафика, напротив, может помочь идентифицировать конкретного пользователя.

Так что «готовить» современные VPN, прицеливаясь на «приватность», нужно особенно тщательно (а лучше считать, что приватности там нет).

Интересно, что развитие, соответствующее построению всё новых и новых туннелей, оказывается не таким уж и односторонним. Например, в части сервисов DNS уже достаточно давно произошло обратное «просачивание» адресов через слои протоколов: технология под названием EDNS Client Subnet (ECS) позволяет резолверу передать в сторону авторитативного сервера сведения об IP-подсети клиента, который обратился с запросом. То есть авторитативный сервер увидит IP-адресный блок, который соответствует клиенту, находящемуся за резолвером, и это позволит определить провайдера. ECS поддерживается, например, Google Public DNS (и не только). Предполагается, что авторитативный сервер, определив провайдера клиента резолвера, как раз и сможет применить какие-то правила оптимизации. Можно представить, что даже если VPN используется для сокрытия IP-адреса пользовательского подключения, но DNS-сервис напрямую обслуживает DNS-запросы, то наличие ECS в этом DNS-сервисе позволит авторитативным DNS-серверам узнать исходную подсеть. Пример хорошо иллюстрирует принципы перемешивания логики между уровнями и протоколами, но тоже вряд ли соответствует ожиданиям относительно «приватности подключения».

Один из стратегических выводов, которые можно сделать, наблюдая за «прорытием» всё новых и новых туннелей-протоколов, такой: в ближайшей перспективе возможно разделение большой Сети не только на «региональные сегменты», но и на интернеты «уровня приложений». Так, возможное инкапсулирование внутрь туннелей систем адресации (что отчасти намечено в ECH) грозит возникновением дополнительной «маршрутизации» (в принципе, такие решения сегодня имеются внутри крупнейших провайдеров уровня Google). Пользователь станет подключаться через выбранное приложение к некоторой условной наложенной сети, в которой ему будет выводиться представление Интернета, собранное через прокси и точки выхода того сервиса «приватности», к которому этот пользователь подключается. А снаружи останется динамическое перемешивание сессий между уровнями, как основной способ сокрытия не только состава трафика, но и самого факта доступа к каким-то внешним ресурсам. На десктопе в качестве вероятного способа технической реализации можно отметить сочетание браузера и встроенного в браузер VPN-клиента от соответствующего поставщику браузера VPN-сервиса.

Немалое значение для возникновения перемешивающих туннелей имеет и такая особенность современного Интернета, как изменяющаяся прозрачность относительно разных протоколов. Речь о том, что из конца в конец подключения могут доходить отдельные пакеты, но при этом промежуточные узлы-инспекторы не пропускают трафик конкретного протокола. То есть, если в простом случае признаком для блокирования мог являться IP-адрес, сочетание IP-адреса с номером порта, то более развитые системы смотрят на контекст сессии, который находится выше уровня пакетов (DPI), и действуют по признакам обнаружения высокоуровневых (относительно IP) протоколов, будь то, к примеру, OpenVPN или TLS заданной версии с подозрительными ECH-расширениями.

Раньше подобные решения встречались на рубежах корпоративных сетей, а не в «межсетевом» пространстве, как сейчас. Причём влияние «промежуточных коробочек» (middle boxes), рассматриваемых как «чёрный ящик», проявляется разными способами, иногда весьма техничными. Так, в спецификации TLS 1.3 сохранился совершенно бесполезный для данной версии сигнал ChangeCipherSpec (CCS), который «промежуточные коробочки» в предыдущих версиях могли использовать в качестве признака установленной TLS-сессии, не пропуская, таким образом, TLS-трафик версии 1.3 без CCS. То есть в новый протокол добавили пустой сигнал (в 1.3 CCS игнорируется) только для того, чтобы последовательность флагов соответствовала сложившимся сигнатурам «обобщённого TLS». Это пример подхода, когда «что-то непонятное» не пропускает промежуточный узел-фильтр, а пропускает только те сессии, для которых удалось обнаружить сигнатуру.

С одной стороны, современный полностью зашифрованный протокол туннелирования может быть спроектирован так, что его сессии не будут иметь сигнатур вообще: при наличии общего секрета на двух сторонах создаваемого туннеля даже процедуры аутентификации и согласования параметров могут выглядеть как обмен пакетами (например, UDP) случайной длины со случайными данными внутри. С другой стороны, если промежуточные узлы пропускают только трафик с сигнатурой по списку, такая неизвестная сессия обречена на прерывание, но, скорее всего, не на первых пакетах. Как раз этот момент и создаёт базу для использования — при создании совсем уж специальных туннелей — протоколов, внешний вид трафика которых вычислительно неотличим от случайных пакетов (что бы это ни значило). А те варианты доступа к скрытым сервисам, которые создаются в надежде на длительные сессии с непрерывным и широким потоком данных, вынуждены вкладываться в протоколы с хорошо узнаваемыми сигнатурами (типа TLS в варианте HTTPS).

Сегментация современной глобальной Сети происходит не только в параллельных плоскостях, находящихся на разных уровнях (привычные транспорты и приложения, работающие поверх них), но и в «перпендикулярных плоскостях», когда протоколы туннелируются между транспортами через приложения. Но это добавляет сложности для всех сторон, участвующих в процессе. Технологии туннелирования набирают популярность. Теперь это не просто некие «обобщённые VPN», но и DNS-over-TLS, DNS-over-HTTPS, а также другие решения из разряда ECH, прямо связанные с уровнем приложений. В области VPN и туннелей растёт распространённость скрытых точек входа и скрытых сервисов. Всё это создаёт новые измерения для перемешивания логики соединений, а привычный описательный подход «узел-канал-узел» больше не работает.

Литература:

[1] https://blog.cloudflare.com/announcing-encrypted-client-hello/
[2] https://groups.google.com/a/mozilla.org/g/dev-platform/c/uv7PNrHUagA/m/BNA4G8fOAAAJ
[3] https://chromestatus.com/feature/6196703843581952
[4] https://tcinet.ru/press-centre/articles/7563/
[5] https://ii.org.ru/dns-kak-istochnik-globalnoy-informacii-o/

Об авторе:

Александр Анатольевич Венедюхин, ведущий аналитик Фонда развития сетевых технологий «ИнДата»

Облака в космосе

Владимир Глебский

В статье рассматривается проблематика развития современных систем передачи и обработки данных с использованием спутниковых каналов связи и датацентров. Проекты в этой области множатся и реализуются различными группами операторов и характеризуются высокой степенью взаимной интеграции облачных и космических технологий в интересах получения услуг передачи и обработки данных принципиально нового качества.

Наверное, одной из самых экзотических является тема создания облачных платформ в космосе, вернее, по-крупному ее можно разделить на два основных направления:

- создание космических центров хранения и обработки данных (ЦОД);
- создание космических сетей и услуг для облачных платформ на Земле.

Естественно, ничто не мешает их взаимной интеграции, и, безусловно, такое взаимодействие вместе с соответствующими сервисами сложится по мере реализации различных проектов в этой сфере, но их особенности удобнее рассматривать по отдельности, как и сами проекты.

Нужно сказать, что если второе направление реализуется преимущественно на базе уже существующих спутников, линий связи, технологических решений и предоставляющих их компаний, а значит, и риски в этих проектах должны быть умеренными, то первое требует создания принципиально новых космических аппаратов и сетей связи и выполняется оно компаниями-стартапами, со всеми вытекающими из этого последствиями.

Первый вопрос, который чаще всего возникает, – в чем смысл использования космоса как среды для облачных платформ? Неужели на Земле не хватает места и ресурсов для ЦОД или космические линии связи лучше наземных?

Вопрос имеет под собой все основания, тем более что практически все проекты в этих направлениях находятся в стадии разработки и апробирования, и точно сказать об их конечной результативности можно будет только в будущем. Но уж больно серьезные игроки рынка взялись за эту тему, чего только стоят имена таких гигантов облачных вычислений, как Amazon, Microsoft и Google. Но не так все просто.

Действительно, космическая среда вовсе не подарок и сулит как опытным игрокам, так и стартаперам много сюрпризов. Энтузиасты облачных космических проектов говорят о том, что в космосе пока нет арендной платы за размещение объектов, электричество можно получать от солнца чуть ли не даром, до самих объектов сложно добраться и нельзя физически похитить данные, а скорости каналов связи, особенно в оптическом диапазоне, будут поистине космическими! Масса плюсов! Космос – это технологично, дешево, надежно, перспективно! Но, увы, в космосе достаточно «дёгтя», способного испортить не одну бочку «облачного меда».

Во-первых, орбиты, на которых планируется размещать космические ЦОД и на которых уже летают спутники, обеспечивающие передачу данных высокоскоростного Интернета, к сожалению, зарастают космическим мусором. И если физически похитить данные прямо в космосе действительно сложно, то физически повредить космический ЦОД или спутник связи вполне можно. С ростом количества мусора медленно, но неуклонно растет и вероятность повреждений. Те, кто разрабатывает эти системы, знают об этом, и для увеличения надежности включают в проекты дополнительные резервные ЦОД и спутники, а это удорожает стоимость системы в целом. Причем касается это как геостационарной, так и средних и низких орбит. К тому же, чтобы данные из космического хранилища попали к потребителю на Земле, они должны пройти по защищенным каналам спутниковой связи, их нужно принять и обработать в специализированном наземном центре, а затем передать по наземным каналам до устройства клиента. Вся эта наземная инфраструктура тоже должна быть надежно защищена от повреждения и нарушения целостности данных.

Во-вторых, для обеспечения каналов передачи данных, действительно сопоставимых по характеристикам с высокоскоростными наземными, спутники должны размещаться как можно ближе к потребителю, проще говоря, к Земле, а это низкие орбиты от 1000 км и ниже, иначе задержки в получении сигнала из облака испортят всю радость от его безопасного размещения. К сожалению, объекты на этих орбитах живут около 3-5 лет, а это значит, что, к примеру, ЦОД вам придется обновлять на орбите каждые 3-5 лет! Тогда как на земле он стоит десятилетиями, да еще и модернизируется. Не говоря

уж о том, сколько стоит запуск каждого килограмма на орбиту. Экономика получается совсем другая.

В-третьих, если получение энергии от Солнца через солнечные батареи — вопрос давно отработанный (хотя цена этих батарей, срок их службы, экологичность их производства — это отдельная тема), то вот рассеять тепло, образующееся в процессе работы ЦОД или другого космического «железа», это большая проблема. Космос не океан, толща которого может забрать на себя огромное количество тепла (хотя и по этому поводу я предвижу громкие крики экологов и климатологов: «Долой!»), в космосе энергию можно «отдать» только через тепловое (инфракрасное) излучение. Попросту говоря, большой ЦОД в космосе должен иметь огромные радиаторы, и они не могут находиться «друг за другом», а должны располагаться по поверхности, чтобы не отдавать тепло друг другу, что делает такой ЦОД похожим на огромное тело, практически пустое внутри или же заполненное элементами с эффективным теплоносителем, отводящим тепло от центральных частей наружу. Запустить и собрать такую конструкцию в космосе — отдельная инженерная задача. Собственно, поэтому в действующих проектах речь идет не о полноценных крупных ЦОД, а о системах микро- или мини-ЦОД с распределенными в них мощностями. Многие, наверное, помнят, сколько было шума из-за яркого свечения групп спутников системы StarLink, мешающего астрономическим наблюдениям, представьте теперь себе на соседних с ними орбитах объекты в сотни раз большего размера!

Существуют в космосе и такие неприятные вещи, как вспышки на Солнце и радиация, выводящие аппаратуру спутников из строя. Список отрицательных сторон можно продолжать и дальше.

Проще говоря, реализация проектов космических облачных платформ осуществима с учетом существенного количества самых разных ограничений, каждое из которых создает свои группы рисков.

Начнем с серьезных игроков облачного рынка. Что же привлекло в космосе Amazon, Microsoft и Google?

На самом деле они не ищут рисков и экзотики, а действуют вполне прагматично. Глобальные задачи, которые они пре-

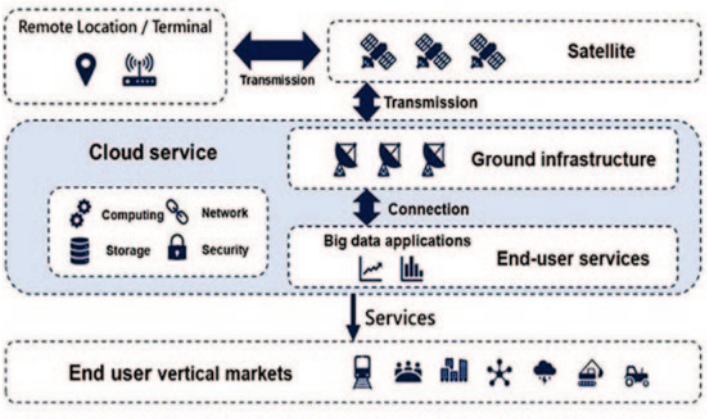


Рис. 1. Схема организации доступа терминала клиента к облачной платформе и предоставляемым ею услугам через спутники.

Рис. 2. Наземная станция проекта AWS Ground Station, обеспечивающая взаимодействие клиентов со спутниками и облачной платформой.

следуют, — это удовлетворить растущие потребности своих действующих клиентов, привлечь к своим облачным сервисам новых клиентов, занять свободные ниши рынка и обеспечить свою конкурентоспособность.

К примеру, Amazon в настоящее время продолжает реализовывать проект AWS Ground Station, в рамках которого создал и развивает собственную наземную сеть спутниковой связи, с ее помощью обеспечивая своим клиентам доступ к облачной платформе Amazon Web Services (AWS). Это, прежде всего, те потребители, для которых доступ к AWS по наземным сетям связи ограничен или невозможен в силу недостаточности или отсутствия соответствующей наземной инфраструктуры, а также широкий спектр потребителей, которые заинтересованы в максимально быстром внедрении облачных технологий как в свои собственные технологические процессы, так и в пакеты предоставляемых ими сервисов для клиентов. Однако создавая свою сеть наземных спутниковых станций, Amazon вступает в конкуренцию с другими операторами спутниковых услуг, и эти вложения носят довольно рисковый характер, так как на данном рынке активно работает внушительное число специализированных предприятий. Помимо этого, Amazon приступил к реализации проекта Project Kuiper – создания своей низкоорбитальной спутниковой сети высокоскоростного доступа в Интернет из 3236 аппаратов, по сути, будущего конкурента сети Starlink Илона Маска. Таким образом, Amazon идет по пути создания собственной полносвязной спутниковой инфраструктуры, пытаясь расширить спектр уже оказываемых услуг, а также открыть для себя новый сектор услуг спутникового широкополосного доступа в Интернет и услуг Интернета вещей (IoT).

Компания Microsoft реализует проект вычислительной платформы, предназначенной для обработки и хранения данных, получаемых от спутников Земли – Azure Orbital. По сути, это расширение облачной платформы Microsoft Azure, запущенной в 2010 году (до 2014 года она носила название Windows Azure), которое предоставляет потребителям возможности наземной спутниковой станции «в формате услуги» (Ground Station As-a-Service, GSaaS). Этот сервис позволяет потребителям обмениваться данными с космическими аппаратами или группировками спутников, а затем обрабатывать эту информацию с использованием облачных хранилищ и вычислительных комплексов. Через платформу

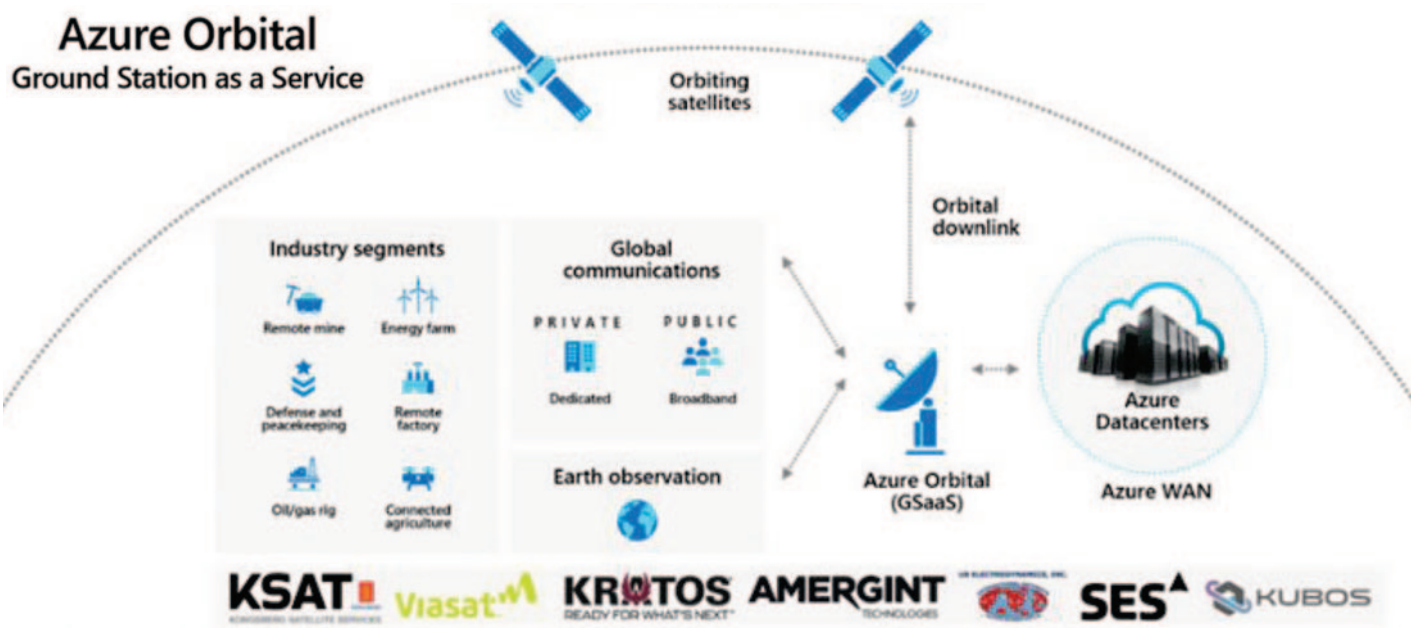


Рис. 3. Инфографика проекта Microsoft Azure Orbital.

клиенты получают доступ к данным спутников различного предназначения, включая спутники связи, наблюдения и дистанционного зондирования Земли.

Нужно сказать, что для реализации проекта Microsoft, в отличие от Amazon, построившего свою наземную инфраструктуру, использует наземные спутниковые станции партнеров – операторов спутниковых систем, таких как Viasat, SES, KSAT и др., владеющих крупными группировками спутников и сетями наземных спутниковых станций, тем самым не вступая с ними в конкуренцию, а напротив, стремясь сделать их своими клиентами и сформировать для них новый сектор специализированных вычислительных услуг. В числе последних к проекту также присоединилась корпорация Space-X, владеющая многоспутниковой системой низкоорбитальных спутников распространения высокоскоростных потоков Интернета Starlink, которая объявила, что видит свою миссию в том, чтобы инновационные решения устраняли барьеры на пути доступа общественных и частных компаний в космическое пространство. Эти амбициозные планы предполагают, что платформа Azure Space должна сделать совместимость и вычисления в космосе более достижимыми для таких отраслей, как сельское хозяйство, энергетика, телекоммуникации и управление, тем самым еще больше внедряя услуги облачных платформ в мировую экономическую систему. Спутниковый оператор SES объявил, что Microsoft станет первым облачным провайдером работающей на средней околоземной орбите группировки O3b mPOWER. В рамках глобальной инициативы Azure Space компания Microsoft вместе со SpaceX, спутниковым оператором SES, компаниями KSAT, Viasat и US Electrodynamics разрабатывает решения, связывающие космические и наземные объекты, в том числе дата-центры. Использование облака MS Azure позволяет хранить и анализировать огромные объемы данных для контроля орбит коммерческих спутников и наблюдения за космическим мусором.

В отличие от Amazon и Microsoft, Google не инвестирует средства в спутниковые системы, а прагматично развивает свою Google Cloud Platform с прицелом на обработку спутниковых данных и различных геосервисов в кооперации с облачными услугами. К примеру, тот же SpaceX активно использует Google Cloud для обработки данных с низкоорбитальных спутников Starlink. Как и конкуренты, Google стремится расширить спектр своих услуг за счет различной информации и данных, получаемых из космоса, но с минимальными для себя рисками.

А что же делают стартаперы, занимающиеся развитием первого направления, о котором мы говорили в начале статьи? Что представляют из себя их спутники и ЦОД?

В традиционных спутниках программное обеспечение (ПО) создавалось для специализированного серверного оборудования космических объектов, так называемых бортовых машин. Использование стандартного серверного оборудования позволяет применять обычное коммерческое ПО, в том числе средства виртуализации и облачные платформы, и перейти к программно определяемым гиперконвергентным системам, дающим возможность разным компаниям совместно использовать орбитальные вычислительные ресурсы и программно перепрофилировать спутники для своих задач. В частности, они могут создавать периферийные edge-облачка для совместной эксплуатации спутника несколькими пользователями, например, для обработки данных спутниковой съемки или мониторинга распределенных датчиков для приложений Интернета вещей.

Появились стартапы, занимающиеся созданием спутниковых микро-ЦОД. В 2019 году калифорнийская компания Vector анонсировала планы запуска программно определяемого спутника GSky-1. Цель проекта, выполняемого совместно с Университетом Южной Калифорнии (USC), – развертывание на микроспутниках облачной платформы Galactic Sky и предоставление космических вычислительных мощностей пользователям по сервисной модели. Легкая ракета-носитель Vector должна была вывести на орбиту созвездие соединенных между собой каналами связи микроспутников, представлявших собою помещенные в прочные контейнеры микро-ЦОД (до 16 виртуальных машин в каждом). Такой

микроспутник-контейнер может кувыркаться, терять связь с Землей, ломаться, но работоспособность одного контейнерного ЦОД не скажется на работе системы в целом. На основе кластера микроспутников с одинаковыми орбитами предполагалось развернуть облачную платформу Galactic Sky.

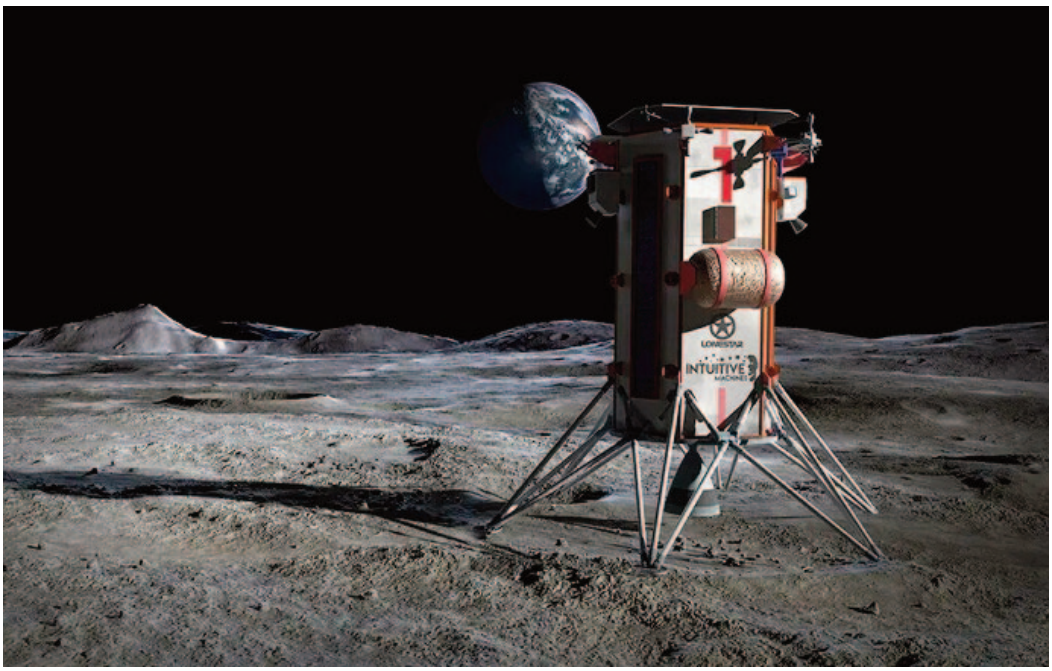


Рис. 5. Лунный ЦОД.

Запланированный на конец 2019 года запуск не состоялся. Но усилия не пропали даром – Lockheed Martin приобрела обанкротившуюся компанию Vector, продолжила сотрудничество с USC и в январе 2022 года все же запустила Gsky-1, правда, под названием Dodona. Компания позиционирует его как первый спутник, использующий программно определяемую спутниковую архитектуру SmartSat. Система работает на платформе NVIDIA Jetson и включает решение для создания приложений искусственного интеллекта NVIDIA JetPack. Системы искусственного интеллекта задействуются для обработки изображений и цифровых сигналов.

В мае 2021 года стартап из Сан-Франциско Loft Orbital в рамках программы инновационных исследований для малого бизнеса получил контракт с Космическими силами США для разработки edge-компьютера, который способен анализировать данные в космосе. Loft Orbital предлагает заказчикам размещать полезную нагрузку на борту своих спутников и управлять ею через веб-портал Cockpit, а также планирует самостоятельно разрабатывать космические сервисы, которые будут предоставляться со спутника по модели SaaS.

Базирующаяся во Флориде компания OrbitsEdge предлагает использовать на орбите модель colocation, монтируя серверы в стандартную 19-дюймовую серверную стойку с объемом для оборудования 5U и подключая их к защищенной от неблагоприятного воздействия космоса запатентованной компанией шине OrbitsEdge SatFrame Constellation. По сути, стандартные серверы будут размещаться в космическом микро-ЦОД.

Рис. 4. Состав подсистем микро-ЦОД.

Разработчики дата-центров смотрят дальше земных орбит и уже планируют разместить их на других космических объектах. Для начала – на Луне. Принимавшая участие в работах на МКС американская компания Lonestar Data Holdings в апреле 2022 года объявила о создании серии ЦОД на лунной поверхности. Компания заключила контракт на два первых полета на Луну и сборку на ней первого дата-центра. Lonestar занимается разработкой сервера, а за проект спускаемого аппарата Nova-C и его посадку отвечает компания Intuitive Machines.

Пилотный «лунный ЦОД» предполагается доставить на поверхность нашего спутника до конца 2024 года и разместить вблизи холмов Мариус в океане Процелларум в вырытой роботами шахте. Активного обмена данными с Землей на первом этапе не планируется – микро-ЦОД, скорее, будет играть роль резервного бэкапа с самой важной и неизменяемой информацией планеты.

Это только ряд примеров различных проектов, нацеленных на использование космоса как среды для развития будущих облачных платформ. Все проекты описать в одной статье невозможно, но надеюсь, мне удалось показать основные направления, проблемы и диапазон задач «космических облаков».

Литература:

https://22century.ru/space/91486?ysclid=lnkfvtg88w970219808
https://3dnews.ru/1081700/amazon-poluchila-razreshenie-regulyatora-na-zapusk-internetsputnikov-project-kuiper
https://www.iksmedia.ru/articles/5924215.html?ysclid=lnkfwlesnj190707276
https://servernews.ru/1084837?ysclid=lnkfs8yr18752427237
https://tass.ru/kosmos/9777767?ysclid=lnkfv143q361626357
https://habr.com/ru/companies/1cloud/articles/439624/

Об авторе:

Владимир Леонидович Глебский, директор отдела развития региональных проектов Международной организации космической связи «Интерспутник».

Облачные сервисы — новая нефть

Алексей Костин

Для бизнеса цифровая трансформация уже несколько лет является одной из самых приоритетных задач и главным элементом стратегии развития, обеспечивающим конкурентные преимущества и значительный бизнес-эффект. В свою очередь облачные технологии являются главным драйвером цифровизации. Сегодня технологии виртуализации развиваются активнее традиционных платформ и позволяют компаниям быстрее достичь технологического прогресса.

Неудивительно, что на этом фоне мировой рынок облачных сервисов в целом и российский рынок в частности стремительно растут, а технологии предоставления быстрого, надежного и безопасного доступа к облачным платформам развиваются. В этой статье мы расскажем о состоянии отечественной отрасли cloud-сервисов, рассмотрим особенности ее развития и разберемся, на что следует обращать внимание заказчикам таких услуг.

Россия поднимается в облака

По данным исследования «Российский рынок облачных инфраструктурных сервисов 2022», проведенного iKS-Consulting, объем услуг российских облачных сервисов в прошлом году достиг 86,6 миллиарда рублей, что на 41,6% больше, чем в 2021 году.

Росту рынка способствовал активный переход корпоративных пользователей с зарубежных сервисов на отечественные облака из-за введенных санкций. В связи с уходом иностранных провайдеров серьезно изменилась конъюнктура рынка облаков: многие российские компании из сегмента малого и среднего бизнеса были вынуждены искать альтернативы западным продуктам.

Помимо увеличения количества клиентов, некоторые компании увеличили и долю рынка за счет повышения стоимости своих услуг. В частности, цены выросли из-за удорожания сетевого и серверного оборудования, а также ухудшения логистики.

Как показало исследование Cloud.ru, в 2022 году российский рынок облачных сервисов вырос на 40% относительно предыдущего года. По мнению авторов, рынок будет демонстрировать рост с похожими показателями и в 2023 году. Сегменты IaaS (инфраструктура как услуга) и PaaS (платформа как услуга) совокупно, а также SaaS (ПО как услуга) в прошлом году выросли на 53% и 42% соответственно. Ожидается, что в текущем году IaaS и PaaS вырастут на 40-45%, а SaaS – более чем на 25%.

Аналитики CorpSoft24 прогнозируют рост облачного рынка в России на 45-50% к концу 2023 года, что сопоставимо с показателями 2022 года. По словам руководителя облачного направления компании Дениса Афанасьева, основным драйвером рынка являются облачные сервисы, предоставляемые по модели IaaS. «Для многих заказчиков они стали эффективным инструментом оптимизации затрат на IT-инфраструктуру в условиях, когда стоимость оборудования резко подскочила, а процедура его закупки усложнилась. От сервиса по модели SaaS заказчику легче отказаться, если речь идет о сокращении расходов», – пояснил эксперт. По его мнению, решения на базе гибридных облаков, контейнеризации и бессерверных облаков не менее перспективны. Вместе с тем Денис Афанасьев предположил, что в сегменте IaaS произойдет консолидация рынка за счет M&A-сделок и ухода слабых игроков, а также появятся новые перспективные участники.

Директор бизнес-юнита «Облачные сервисы» «КРОК инкорпорейтед» Сергей Зинкевич рассказал о дополнительных факторах, которые мотивируют компании переходить в облака. Он ссылается на результаты исследования компании, согласно которым около 70% организаций испытывают различные сложности с поддержанием IT-инфраструктуры. По словам Сергея Зинкевича, спрос на IaaS в этой связи продолжит расти, хотя окажется менее взрывным. На сегодняшний день сегмент PaaS занимает в России самую маленькую долю – около 5%, а спрос на такие услуги только формируется и в ближайшей перспективе будет очень быстро расти.


Изображение от Freepik

По оценке iKS-Consulting, абсолютным лидером рынка в сегменте IaaS по итогам 2022 года является «Ростелеком-ЦОД» с долей 25%. Cloud (раннее название – SberCloud) и Selectel заняли вторую (17,2%) и третью (9,5%) строчку соответственно, опередив МТС (9,3%) и Yandex Cloud (6,3%). При этом почти половина корпоративных клиентов пользовалась услугами сразу нескольких провайдеров, а главным потребителем облаков стал ретейл.

По данным обзора «Облачные сервисы 2023», выпущенного CNews Analytics, список крупнейших поставщиков SaaS в России по итогам 2022 года возглавляет «СКБ Контур» с выручкой 27,5 миллиарда рублей, на втором месте «Тензор» – 10,9 миллиарда рублей, на третьем – Softline с 6,3 миллиарда рублей, четвертую позицию занимает Mango Office – 6 миллиардов рублей, а замыкает топ-5 «Эвотор» с выручкой от SaaS 3,4 миллиарда рублей.

Аналитики iKS-Consulting также утверждают, что в 2023 году более 30% российских предприятий намерены инвестировать в облачную IT-инфраструктуру, рассматривая преимущественно российские сервисы. В общем объеме российского IT-рынка облачные сервисы составляют 5,8% против 13% в среднем на мировом рынке. В 2025 году рынок облачных сервисов достигнет объема более 200 миллиардов рублей.

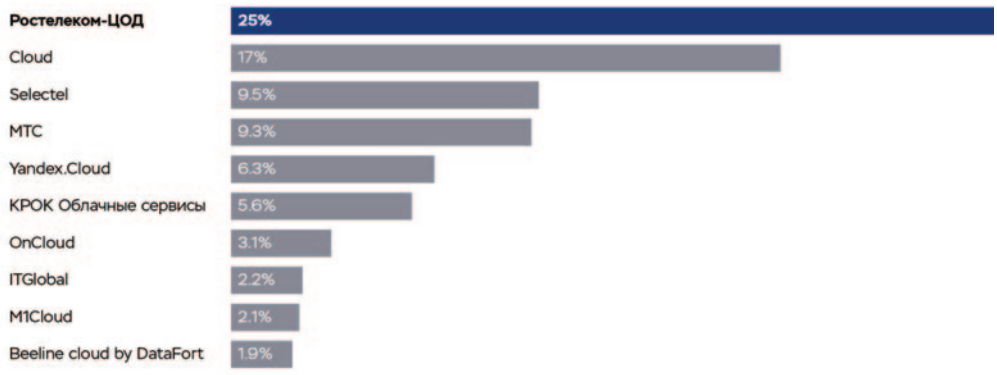


Рис. 1. Топ-10 крупнейших поставщиков IaaS в России в 2022 году по доле рынка.
Источник: IKS-Consulting, включая продукт Bare metal

Учитывая, что в среднем расходы компаний в США на облака в шесть раз превышают расходы российских компаний, возможности спроса имеют кратный потенциал роста.

В текущих условиях развитие рынка облачных сервисов в России стимулирует и государство, которое заинтересовано в сохранении персональных данных россиян внутри страны, обеспечении безопасности критически важной информации и импортозамещении зарубежных решений и сервисов.

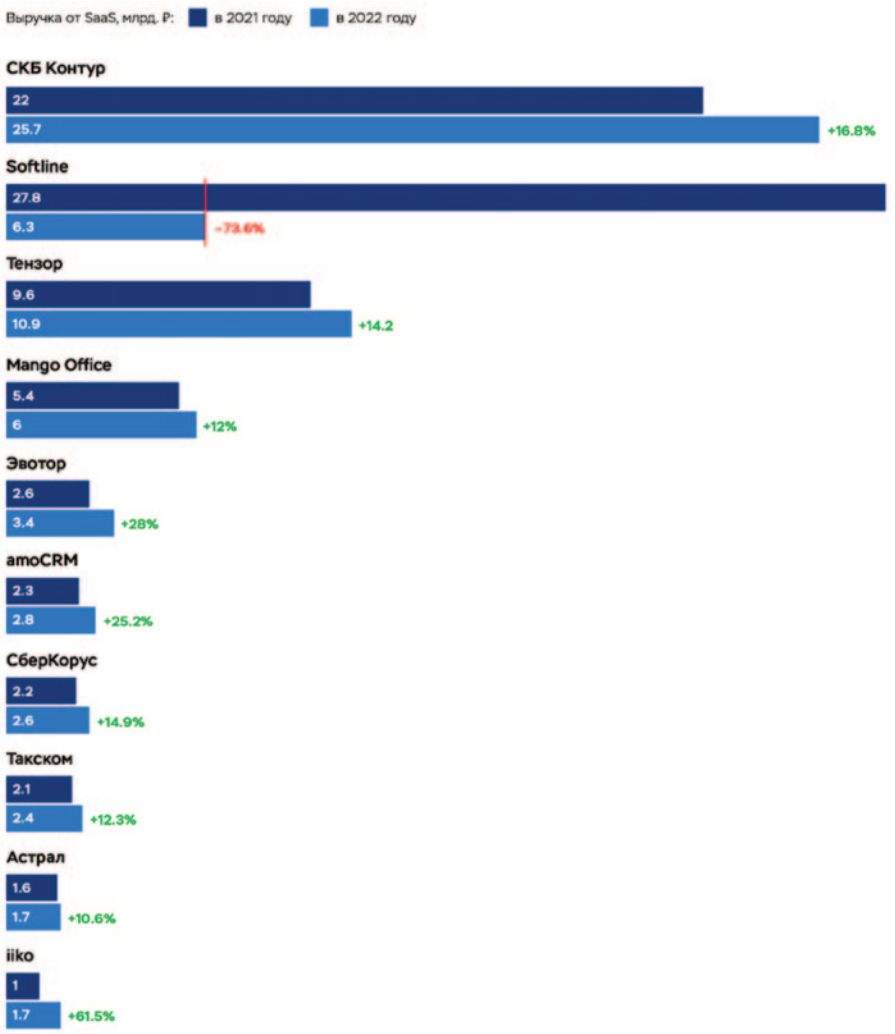


Рис. 2. Топ-10 крупнейших поставщиков SaaS в России в 2022 году по выручке. Источник: CNews Analytics

Весной этого года ситуация на российском рынке облачных технологий стала предметом обсуждения в Совете Федерации. Среди прочего участники круглого стола заметили, что в безопасные отечественные облака стоит мигрировать в том числе частному бизнесу, работающему с чувствительными для государства и граждан данными. Зампред комитета Совфеда по экономической политике Константин Долгов заявил, что в предпринимательской сфере содержится много «чувствительной информации», которую необходимо защищать; в связи с чрезвычайной актуальностью проблемы защиты персональных данных, бизнесу следует активнее мигрировать в безопасные отечественные облака – пусть не в государственные, а в частные, при поддержке регулятора.

Ближайшие тренды

Облачный рынок в России активно развивается в целом, однако в ближайшее время некоторые тенденции будут на нем превалировать.

Первая из них – оптимизация IT-систем. Многие иностранные вендоры оборудования и ПО покинули Россию, ограничили поставки и поддержку лицензий, включая системы хранения данных, серверы и системы защиты информации. Вот почему в 2023 году бизнес будет активно перестраивать IT-ландшафт, оптимизируя вычислительные мощности и программные продукты, чтобы снизить операционные расходы, и концентрируясь на решениях, обеспечивающих непрерывность бизнес-процессов.

Это потребует от бизнеса наращивания экспертизы по миграции в облака, что даст преимущество тем сервис-провайдерам, которые смогут предложить комплексный подход к построению IT-инфраструктуры, в том числе индивидуальный подход к решению IT-задач заказчика.

Вторая тенденция – фокус на облака, созданные на основе импортозамещенного оборудования. 2022 год показал тотальную зависимость российского бизнеса от иностранных технологий, поэтому компании сосредоточатся на управлении IT-рисками, а каждая организация будет искать отечественные альтернативы зарубежным решениям и сервисам, параллельно регулируя проблему совместимости продуктов. Ключевым моментом станет увеличение доли облаков российских сервис-провайдеров в инфраструктуре бизнеса.

Главный тренд, следующий из остальных, – рост спроса на облака. Рынок демонстрирует устойчивость, не столько бьющую по нему, сколько открывающую новые возможности для развития различных сервисов. Основным драйвером роста российских облаков станет локализация IT-отрасли. Российские сервис-провайдеры уже доказали свою состоятельность и надежность, благодаря чему доверие к ним возросло.

По прогнозам Stack Group, к концу этого года доля облаков в IT-инфраструктуре российского бизнеса будет варьироваться от 30% до 100%, при этом инфраструктурные сервисы будут расти быстрее, чем PaaS и SaaS. Облака закроют сразу несколько потребностей заказчиков: позволят автоматизировать работу, снизить операционные расходы и обеспечить безопасность данных.

Информационная безопасность всегда играла очень важную роль, а в нынешней ситуации стала чуть ли не ключевым направлением развития IT. Выбирая облачного партнера, бизнес будет ориентироваться на облачные инфраструктуры с интегрированными решениями по информационной безопасности (ИБ), в том числе из-за повышения требований со стороны законодательства. Далеко не у каждой организации есть возможность держать в штате собственного специалиста по ИБ, а сервис-провайдеры имеют больше возможностей инвестировать в ИБ и предлагать защищенные облачные решения, соответствующие всем текущим требованиям.

Подробнее о безопасности

Облачные интегрированные решения информационной безопасности представляют собой комплексные платформы и сервисы, предназначенные для защиты информации и обеспечения безопасности в облачной среде. Они объединяют в себе различные инструменты и технологии, которые позволяют организациям эффективно реагировать на современные киберугрозы.

Суть облачных интегрированных ИБ-решений заключается в том, чтобы объединить различные аспекты безопасности в одной платформе, которая может быть интегрирована с облачной инфраструктурой.

Основные характеристики таких решений включают несколько составляющих.

Мониторинг и управление ИБ в облачной среде. Позволяет выявлять и анализировать потенциальные угрозы, наблюдать за активностью пользователей, контролировать доступ к данным и ресурсам, а также принимать соответствующие меры по обеспечению безопасности системы.

Аутентификация и управление доступом к облачным ресурсам. Набор инструментов для аутентификации пользователей, управления и контроля привилегий, определения политик безопасности и механизмов идентификации.

Защита данных, хранящихся и передаваемых в облаке. Включает в себя шифрование, контроль целостности, методы резервного копирования и восстановления данных, а также предлагает механизмы обнаружения и предотвращения утечек информации.

Управление угрозами и рисками. Облегчает выявление, анализ и управление угрозами и рисками, связанными с облачными средами. Средства, которые предлагают возможности мониторинга и обнаружения инцидентов, решения для управления инцидентами и реагирования на угрозы, а также инструменты для анализа логов и аудита системы.

Таким образом облачные интегрированные ИБ-решения помогают клиентам улучшить общую безопасность в облаке, обнаруживая и предотвращая угрозы, а также обеспечивая защиту данных и контроль доступа. Также они позволяют сократить риски, связанные с конфиденциальностью данных, и дают возможность обнаружения и реагирования на инциденты быстрее и более эффективно.

Вот несколько самых известных примеров подобных решений от зарубежных поставщиков: Amazon Web Services (AWS) Security Hub, Microsoft Azure Security Center, Google Cloud Security Command Center, IBM Security Connect и Cisco Cloud Security.

Российский рынок ИБ также предлагает несколько облачных интегрированных решений, например:

Kaspersky Security для облачных услуг – решение от Kaspersky Lab, которое обеспечивает комплексную защиту облачных инфраструктур и данных. Оно включает в себя антивирусную защиту, брандмауэр, системы предотвращения вторжений и другие инструменты безопасности.

«Фабрика Защиты» – облачная информационно-аналитическая система, разработанная компанией Positive Technologies. Предоставляет функции по обнаружению и предотвращению кибератак, мониторингу уязвимостей, контролю за соблюдением требований собственности и многим другим.

«Безопасное облачное хранилище Mail.ru» – решение от Mail.ru Group, которое позволяет пользователям хранить и синхронизировать свои данные в облаке с максимальной степенью защиты. Включает функции шифрования, двухфакторной аутентификации и другие меры безопасности.

Summit Platform – облачная платформа компании Group-IB, предоставляющая ряд инструментов для мониторинга и обнаружения киберугроз. Включает в себя модули обнаружения инцидентов, анализа угроз и реагирования на инциденты в реальном времени.

Это лишь несколько примеров российских облачных ИБ-сервисов. Отечественный рынок активно развивается и на нем появляются новые решения, соответствующие современным требованиям безопасности данных и облачных сервисов.

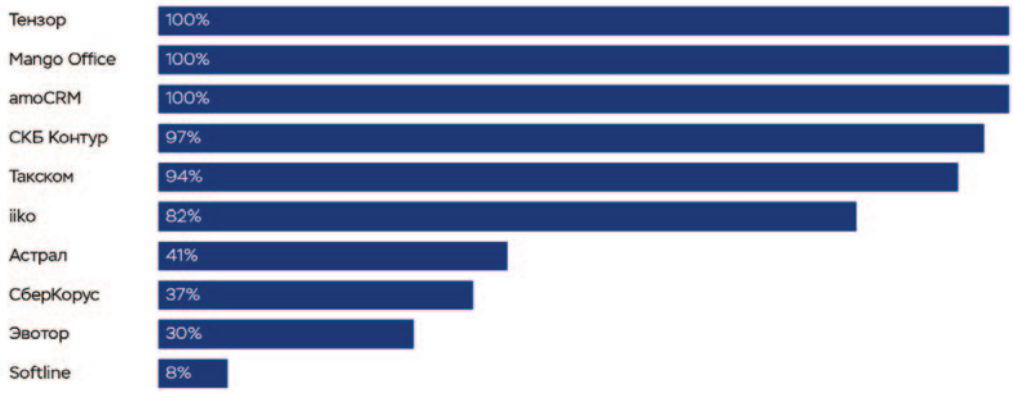


Рис. 3. Доля SaaS в совокупной выручке среди поставщиков в 2022 году.
Источник: CNews Analytics

Технический директор компании MSK-IX Александр Ильин отметил, что облачные решения позволяют эффективно масштабировать и резервировать инфраструктуру, непрерывно обновлять системы без значительных простоев, помогать противодействовать DDoS-атакам и обеспечивать высокий уровень защиты данных. «Благодаря облачным решениям, компании могут распределить свою информацию, снижая риск ее потери и повышая ее доступность для заказчиков», — подытожил Александр.


Изображение от Freepik

Облака всем бизнесам покорны

В целом облачной инфраструктурой могут пользоваться компании из любой отрасли, но круг задач, которые они решают, и используемые ими инструменты будут отличаться. Тем не менее, отрасль может повлиять на выбор типа облака.

Технический директор Selectel Кирилл Малеванов отмечает, что крупные промышленные, строительные, финансовые и медицинские компании, а также телеком-провайдеры чаще выбирают частные облака. Иногда большие компании строят собственные приватные облака на мощностях провайдера. К примеру, компания X5 Group реализовала проект, для которого Selectel как сервис-провайдер подготовил весь необходимый IT-фундамент (серверы, сетевое оборудование и т.д.), а разработчики и архитекторы X5 Group построили на этой инфраструктуре облако для собственных нужд.

Вообще же в Selectel фиксируют наибольший спрос именно на Bare metal – выделенные серверы в облачной среде и аренду вычислительных ресурсов в облаке. Так, за первое полугодие 2023 года выручка сегмента «Приватные облака на базе выделенных серверов» увеличилась на 33% на фоне роста спроса на серверы произвольных конфигураций со стороны крупных клиентов. Выручка сегмента «Публичные и приватные облака» выросла на 44% преимущественно за счет повышенного спроса на сервисы облачной платформы Selectel.

«При этом направление «Услуги дата-центров», куда входит предоставление места в ЦОД в аренду, выросло на 21%, но приносит всего 12% выручки компании», – уточнил Кирилл Малеванов.

Yandex Cloud, один из крупнейших провайдеров облачных услуг, исследовал, как этот сектор рынка применяет облака: промышленные гиганты постепенно переносят в них свою инфраструктуру, приложения и данные, сокращая эксплуатационные расходы. По оценке Gartner, к 2027 году более 50% предприятий будут использовать отраслевые облачные платформы для ускорения бизнес-процессов. При этом российские промышленные компании все еще находятся на ранних этапах облачной трансформации, только тестируя технологию и высчитывая эффекты от оптимизации расходов на IT-инфраструктуру.

По словам директора по работе с промышленными компаниями в Yandex Cloud Павла Приедитиса, глобальные промышленные компании – одни из наиболее активных пользователей цифровых технологий. Производство – непрерывный процесс, поэтому такие компании наиболее требовательны к стабильности, надежности и отказоустойчивости ПО. «В России промышленные предприятия только начинают использовать облачные платформы, хотя уже понимают их преимущества для хостинга сервисов, безопасной разработки и глубинной аналитики данных», – рассказал он.

Количество клиентов Yandex Cloud в первом полугодии 2023 года выросло до 27,9 тысячи. Выручка Yandex Cloud увеличилась в 1,8 раза по сравнению с аналогичным периодом прошлого года и составила 5,8 миллиарда рублей.

«Банки, ретейл и IT-компании лидируют по объемам потребления облачных технологий. Они не только наращивают использование сервисов, к которым обращались изначально, но и по мере роста экспертизы продолжают добавлять в свой IT-ландшафт все новые технологии. При этом радует тенденция, что и более консервативные отрасли продолжают рост опережающими темпами», – прокомментировал коммерческий директор Yandex Cloud Александр Черников.

Директор по развитию «КРОК Облачные сервисы» Сергей Зинкевич отметил тенденцию, согласно которой переход в облака наблюдается среди организаций из секторов экономики, ранее не проявлявших к ним большого интереса. Например, помимо традиционных лидеров по их потреблению – ретейла, банков и IT – отмечается значительный рост интереса со стороны ТЭК, страховщиков, телеком-компаний, медицинских организаций и агропромышленного комплекса (АПК).

Так, главной проблемой АПК является уход зарубежных IT-поставщиков, поэтому агрохолдинги активно ищут российские аналоги. По данным КРОК, 73% агропромышленных компаний ждут от внедрения облачных технологий снижения операционных расходов, 66% – увеличения скорости и гибкости бизнес-процессов, 53% – повышения производительности труда. Предпочтение отдается тем, кто способен перенести инфраструктуру в отечественные облака максимально бесшовно, сохранив эффективность бизнес-процессов и предложив пути ее повышения.

В транспортном секторе востребованы ИИ-технологии для управления логистикой, решения для облачной аналитики и работы с данными пассажиров.

Интерес ретейл-сетей к облачным сервисам объясняется большим объемом данных, которым они оперируют: информацией о продажах, покупателях, движении товаров. Генеральный директор «Infoline-аналитики» Михаил Бурмистров назвал именно этот сегмент крупнейшим потребителем облачных услуг.

Сила облаков

Ранее я упомянул, в чем заключаются преимущества использования облачных технологий – теперь сосредоточимся на главных из них.

Гибкость и масштабируемость. Облачные технологии позволяют быстро масштабировать ресурсы в соответствии с потребностями бизнеса. Предоставляются гибкие опции по выбору ресурсов, таких как вычислительная мощность, хранилище данных и сетевая пропускная способность.

Удобство доступа и мобильность. Облачные сервисы позволяют получать доступ к данным и приложениям из любого места и с любого устройства с подключением к Интернету. Это облегчает командную работу и удаленное сотрудничество, а также увеличивает мобильность пользователей.

Экономическая эффективность. Облачные решения позволяют снизить затраты на аппаратное обеспечение, его обслуживание и обновление. Предоставление IT-ресурсов как услуги позволяет компаниям платить только за использованные ими ресурсы, а не за наличие физического оборудования.

Инновационность и возможность использования передовых технологий. Облачные провайдеры активно разрабатывают и внедряют передовые технологии, такие как машинное обучение, искусственный интеллект и аналитика данных, которые предприятия могут использовать для улучшения своих процессов и разработки новых продуктов и услуг.

Несмотря на то, что все перечисленные пункты имеют большое значение, на сегодняшний день наибольшую актуальность представляют следующие три.

Улучшенные возможности для совместной работы и обмена данными. Облачные платформы предоставляют возможность легко наладить совместную работу и обмен данными между сотрудниками и пользователями как внутри одной организации, так и между различными компаниями. Облака упрощают совместную работу над проектами, обеспечивают единое хранилище для данных и позволяют быстро и эффективно делиться информацией.

Безопасность и надежность. Ведущие облачные провайдеры обеспечивают высокую степень защиты данных и информационную безопасность. Они инвестируют в передовые технологии шифрования, контроль доступа и мониторинг угроз для предотвращения утечек и несанкционированного доступа к данным.

Непрерывная работа и восстановление после сбоев. Провайдеры облачных услуг обеспечивают резервное копирование данных и системы, а также механизмы восстановления после сбоев. Это позволяет минимизировать время простоя и обеспечивает непрерывность бизнес-процессов.

В приведенном перечне были рассмотрены лишь некоторые из преимуществ облачных технологий. В зависимости от конкретных потребностей и сферы деятельности компании их преимущества могут быть еще более разнообразными и значительными.

Без коннекта никуда

Чтобы клиенты облачных сервисов могли оценить все их преимущества и в полной мере удовлетворить свои запросы и ожидания, необходимо выполнить несколько важнейших условий: доступность, связность и безопасность. Решить эти задачи помогает технология Cloud Connect, или как ее еще называют, Direct Cloud.

Это технология, которая предоставляет прямое и безопасное соединение между локальной инфраструктурой организации и провайдерами облачных услуг. Для доступа к облачным ресурсам обычно используется Интернет, но такое соединение может быть нестабильным, неэффективным в случае больших объемов данных или при наличии строгих требований к низкой задержке и высокой пропускной способности, а также – что очень важно – небезопасным.

Cloud Connect предоставляет прямое физическое подключение между организацией и облачным провайдером в рамках их собственных сетей или через третью организацию, которая обеспечивает это соединение для более надежной и быстрой передачи данных между организацией и облачным окружением.

Преимущества использования Cloud Connect включают повышенную безопасность, низкую задержку, гарантированную пропускную способность и лучшую производительность для приложений, работающих в облаке, сохраняя при этом контроль над данными и приложениями. Кроме того, это может снизить расходы на сетевые соединения и повысить гибкость в управлении ресурсами.

Это особенно полезно для организаций, которые имеют высокие требования к безопасности данных или осуществляют передачу больших объемов информации между своими внутренними системами и облачной инфраструктурой.

Услуги Cloud Connect предлагают многие международные компании, обеспечивающие прямое соединение между облачными провайдерами и организациями.

Так, Amazon Web Services (AWS) с услугой AWS Direct Connect предоставляет прямое соединение между клиентами и инфраструктурой AWS. Microsoft Azure ExpressRoute обеспечивает высокоскоростное, надежное и частное соединение между клиентской инфраструктурой и облаком Microsoft Azure. Google Cloud Interconnect предоставляет возможность прямого соединения синхронной и асинхронной передачи данных между клиентами и облачной инфраструктурой Google Cloud. IBM Direct Link позволяет клиентам соединяться непосредственно с облаком IBM Cloud, обеспечивая надежное и высокоскоростное прямое соединение. Equinix предлагает услугу Cloud Exchange, которая позволяет клиентам подключаться ко множеству облачных провайдеров через их глобальную платформу дата-центров.

В России также работают различные провайдеры услуги Cloud Connect. Например, MSK-IX предлагает услугу Cloud Connect в рамках своей платформы Instanet. «Мегафон» обладает одной из крупнейших мобильных сетей в России и также предоставляет услугу Cloud Connect через свою об-

лачную платформу «Мегафон Облако». Компания DataLine, специализирующаяся на предоставлении услуг облачного хостинга и колокейшна, также предлагает услугу Cloud Connect через свою облачную платформу. Провайдер облачных услуг и инфраструктуры Selectel предоставляет услугу Direct Connect для организации связи клиентов как с облачной платформой на базе сети собственных дата-центров, так и с зарубежными провайдерами с помощью защищенного канала. «Яндекс» выступает на этом рынке с услугой Yandex Cloud Interconnect – сервисом для создания выделенных сетевых соединений между локальной инфраструктурой и Yandex Cloud.

Это далеко не полный список компаний, предоставляющих услугу Cloud Connect в России, но он дает представление о разнообразии и масштабе рыночных игроков. На первый взгляд может показаться, что принципиальных различий между перечисленными компаниями нет, а их сервисы весьма схожи. Между тем следует принимать во внимание нюансы.

Во-первых, мы по понятным причинам для начала отсекаем зарубежных поставщиков услуг. Во-вторых, если внимательно присмотреться, можно заметить, что большинство компаний обеспечивают прямое соединение клиентов только с собственной облачной платформой – например, Yandex Cloud. Если же заказчик использует сервисы от других поставщиков, такой вариант ему не подходит. Другие провайдеры агрегируют на своей платформе услуги от различных облаков, однако их перечень так или иначе ограничен, как ограничено и количество телеком-операторов, подключенных к платформе, а также география присутствия провайдера. Другими отягчающими факторами могут являться скорость подключения к Cloud Connect, сложность настройки и поддержки услуги.

Вот почему во избежание подобных проблем в качестве поставщика услуги следует выбирать независимого инфраструктурного оператора с максимально широкой географией присутствия и высоким уровнем экспертизы – своего рода «оператора для операторов».

Например, компания MSK-IX является крупнейшим пиринговым провайдером в России, обладает распределенной сетевой инфраструктурой, точками подключения во всех федеральных округах страны и огромной клиентской базой. К сети MSK-IX подключены все крупные операторы связи, включая «большую четверку», а также ведущие контент-провайдеры и облачные платформы, что дает возможность предоставления услуг по модели MultiCloud, когда клиентам предоставляется возможность подключения к сервисам не одного, а сразу ряда ведущих поставщиков облачных услуг. При этом при подключении через Cloud Connect организуется выделенный канал связи. Таким образом, передача данных не зависит от маршрутизации в публичной сети Интернет, что обеспечивает защиту от внешних угроз. Кроме того, подключение к услуге Cloud Connect занимает от одного дня с момента подачи заявки.

В этом году Selectel и MSK-IX заключили договор о сотрудничестве в рамках услуги Cloud Connect. По словам Кирилла Малеванова, это позволит эффективнее использовать облачные сервисы Selectel, так как клиенты получают доступ к персонализированным решениям для хранения и обработки данных, а также выполнения других бизнес-задач. При этом обеспечивается высокий уровень безопасности и защиты информации, что является важным требованием для большинства компаний.


Изображение от Freepik

«Совместное решение устраняет возможные проблемы с доступностью, стабильностью и скоростью интернет-соединения, с которыми могут сталкиваться пользователи корпоративных облачных сервисов. При этом инфраструктура клиента может находиться в различных регионах России», – добавил технический директор Selectel.

Заключение

По словам генерального директора компании MSK-IX Евгения Морозова, облачные технологии стали неотъемлемой частью современного бизнеса, они активно развиваются и демонстрируют свою эффективность. «Однако, среди всех технологических трендов, мы не должны забывать о важности сетевой связности. Для гарантированного доступа к облачным сервисам необходимо обеспечить быструю и надежную передачу данных по выделенным каналам, не зависящим от маршрутизации в сети Интернет, между сетями заказчиков и платформами облачных провайдеров. Это будет являться одним из ключевых факторов успеха, предоставляя значительные преимущества и возможности для развития цифровых сервисов организации и ее бизнеса в целом», – подчеркнул Евгений Морозов.

Нет никаких сомнений в том, что российский рынок облаков в ближайшее время будет набирать обороты, наращивая количество сервисов и пользователей из различных секторов экономики. В этой ситуации в выигрыше останется тот, кто сумеет оседлать волну и будет располагать наибольшим портфелем услуг, соблюдая при этом важнейшие заповеди: доступность, связность и безопасность.

Об авторе:
Алексей Владимирович Костин, директор по продуктам и маркетингу MSK-IX, a.kostin@msk-ix.ru

Метод сквозной аутентификации пользователей в системе поддержки проведения научно-технических экспертиз

Александр Белов,
Александр Антышев,
Маргарита Гевондян

Научно-исследовательские и опытно-конструкторские работы являются решающим фактором, двигающим мировой технологический прогресс и способствующим новым технологическим и научным инновациям. Инвестиции государственных и частных учреждений, промышленных предприятий в исследования, а также применение передовых технологий играют значительную роль в экономике и процветании страны. Страны, внедряющие инновации путем проведения НИОКР, прилагают значительные усилия в области поддержки компаний и организаций, осуществляющих научные исследования и опытно-конструкторские работы, особенно по прорывным направлениям науки и техники. При этом возникает необходимость предоставления IT-сервисов для компаний и предприятий, претендующих на получение адресной поддержки со стороны государства, а также для государственных органов власти, проводящих научно-техническую экспертизу с целью определения правомерности применения мер поддержки. В статье рассматриваются технологии сквозной аутентификации пользователей для разрабатываемых облачных сервисов поддержки проведения научно-технических экспертиз проектов в области IT.

Введение

Государственная политика импортозамещения в сфере информационных технологий и устранения технологической зависимости от зарубежных разработок продолжается в России уже более 10 лет. Развитие собственной высокотехнологичной промышленности стимулируется правительством через различные правовые механизмы: принятие новых законов с целью улучшения условий для ведения деятельности; финансовая поддержка организаций, осуществляющих деятельность в сфере информационных технологий (предоставление грантов); утверждение льгот в Налоговом кодексе РФ. Наравне с общим уменьшением ставок за аренду территорий и производственных мощностей, существуют методы поддержки и развития наиболее значимых отраслей — IT, научных исследований, экспериментов, инженерно-конструкторских разработок. Внутренние процессы этих производств объединены аббревиатурой НИОКР* (научно-исследовательские и опытно-конструкторские разработки). В случае присвоения такой разработке статуса НИОКР [1] при наличии научной новизны, организация имеет право претендовать на увеличенный бюджет или применить повышенный коэффициент к расходам по налогу на прибыль организаций [2] (т.е. сумму фактических затрат по работам можно увеличить в полтора раза и включить в расходы).

Данная льгота предусмотрена последовательной государственной политикой, ведущейся с 2008 года. Льгота является эффективным рычагом налогового стимулирования инновационной активности с целью создания благоприятных условий для осуществления инновационной деятельности в Российской Федерации при наличии научной новизны для развития национальной науки и техники в целом и устранения технологической зависимости от иностранных разработок и развития собственной высокотехнологичной промышленности [3].

В случае применения указанной льготы налогоплательщик должен представить в налоговый орган отчет о выполненных НИОКР, оформленный в соответствии требованиями, установленными национальным стандартом (Межгосударственный стандарт ГОСТ 7.32-2001) [4].

Налоговые органы осуществляют проверку представленного отчета о выполненных НИОКР по двум направлениям:

- финансовой документации по проекту, заявленному как НИОКР, для определения правильности начисления налогов с учетом применения льготы;
- научно-технического отчета для определения наличия признаков научной новизны и инновационности НИОКР, соответствия выполняемых работ установленным правительством критически важных научно-технических направлений.

Вместе с тем, на практике встречаются случаи, когда налогоплательщики неправомерно применяют льготу, предусмотренную статьей 262 Кодекса, что выявляется в ходе налоговых проверок после назначения и проведения экспертиз специалистами научно-исследовательских организаций и вузов.

Таким образом, экспертиза документации, представляемой IT-компаниями, является важным процессом проверки обоснованности предоставления налоговых льгот не только в России, но и в мировой практике [5].

При проведении НИОКР и подготовке отчетной документации компания, претендующая на предоставление ей налоговых преференций, использует целый ряд цифровых сервисов, таких как система «Антиплагиат» [6], информационно-поисковые системы, реализованные на цифровой платформе Роспатента [7], онлайн-база данных ВИНИТИ РАН и т.п. Эксперты, осуществляющие научно-техническую экспертизу проектов, также используют цифровые сервисы. Процесс проверки отчетной документации инициируют и администрируют налоговые инспекции, используя ведомственные сервисы.

Проведение подобных экспертиз представляет собой многоэтапный процесс, в котором участвуют налогоплательщики, налоговые инспекторы и эксперты. Документация, представляемая на экспертизу, состоит из большого числа текстовых документов, разнообразных как по содержанию, так и по форме. В ряде случаев отчетные документы плохо структурированы, не соответствуют российским и международным стандартам, используют различные форматы. Все это существенно усложняет процесс экспертизы, а выполнение рутинных операций по первичной обработке документов значительно увеличивает ее трудоемкость.

Для повышения эффективности процесса проведения научно-технических экспертиз используются разнообразные автоматизированные системы. Однако все они имеют ярко выраженный отраслевой характер и основаны на анализе текстов с помощью различных NLP-алгоритмов [8, 9]. Зачастую такие системы архитектурно представляют собой монолитные приложения, реализующие функции проверки текста на соответствие эталонной структуре, анализа содержания текста по ключевым словам, выявления заимствований и т.п.

Рассматриваемая в работе система поддержки проведения научно-технических экспертиз [5] разработана на основе требований инспекций Федеральной налоговой службы, компаний-налогоплательщиков, а также представителей экспертного сообщества. К их числу относятся следующие основные требования:

- интеграция с цифровыми сервисами ФНС России;
- интеграция с различными информационными сервисами, предоставляемыми заинтересованными организациями;
- защиту информации, предоставляемой налогоплательщиком;
- возможность заполнения чек-листа налогоплательщиком, а также загрузки отчетных документов, которые предоставляются налогоплательщиком для проведения экспертизы НИОКР, установленного формата;
- многоступенчатый анализ отчетных документов с использованием методов машинного обучения, включая нейронные сети;
- формирование акта экспертизы.

Архитектура системы представляет собой платформенное решение, интегрированное с рядом цифровых сервисов, обеспечивающих проверку отчетной документации о выполненных НИОКР как по форме, так и на предмет их соответствия критерию научной новизны. При этом для налогоплательщиков и экспертов предлагаемое решение будет относиться к типу облачных сервисов SaaS, а для налоговых инспекций – PaaS [10].

Использование пользователями большого количества разнообразных облачных сервисов порождает целый ряд проблем при их эксплуатации и поддержке в рамках интеграционного решения. Одним из наиболее важных вопросов является обеспечение безопасности при использовании интернет-сервисов. Для этого широко применяется технология единого входа, направленная на решение данной проблемы. Технология единого (однократного) входа (англ. Single Sign-On, SSO) – это технология доступа к различным приложениям посредством однократной процедуры аутентификации [11].

Данная технология призвана решить целый ряд задач, в том числе:

- устранение необходимости создания системы регистрации, идентификации и аутентификации пользователя для каждой системы в отдельности;
- объединение ряда систем при помощи единого интерфейса входа, который дает понять пользователям, что они находятся в рамках взаимосвязанной системы;
- технология однократного входа облегчает пользователю процесс использования систем, устраняя путаницу во вводе и запоминании логинов и паролей для каждой системы в отдельности;
- решение такой проблемы дает компании-поставщику услуг в сфере информационных технологий неоспоримое преимущество, позволяя привлекать больше клиентов в несколько существующих систем одновременно.

При проектировании системы были рассмотрены следующие сервисы: Личный кабинет налогоплательщика, «Антиплагиат», Поиск патентов [7]. Каждый ресурс предъявляет собственные

требования к безопасности и определяет собственные процедуры идентификации и аутентификации.

Разрабатываемый подход должен обеспечить возможность формирования системы единого входа для пользователей рассматриваемых сервисов и облегчить их использование. Решение этой задачи проводилось в соответствии со следующими этапами:

- агрегирование всех существующих пользователей с их идентификационными и аутентификационными данными в единый список и создание единого хранилища для него;
- создание универсальной системы идентификации и аутентификации пользователей;
- создание методов и средств для обеспечения связи между сервисом и системой единой идентификации и аутентификации.

Анализ способов аутентификации пользователя

Применительно к RESTful API, как правило, выделяют шесть способов аутентификации (их на самом деле больше):

- Basic;
- Digest;
- Token;
- Certificate;
- Digital signature;
- с применением ключей API (oAuth, oAuth 2.0).

Первый и второй способ используют для доверенных клиентов. Ключи API используют для сторонних клиентов.

Basic-аутентификация

Метод базовой аутентификации — наиболее простой при разработке, но он обеспечивает наиболее низкий уровень защиты, прописанный в опциях протоколов. Чаще всего используется в течение разработки, но не рекомендуется для использования в интегрированной системе [12].

Пример использования: JIRA REST API — Basic authentication.

Digest-аутентификация

Данный метод аутентификации предполагает следующие действия (в случае перехода на страницу, требующую авторизации):

- клиент запрашивает страницу, которая требует аутентифицироваться, но не вводит имя пользователя и пароль;
- сервер отвечает 401 «клиент-ошибка», предоставляя область аутентификации и случайно сгенерированное одноразовое значение;
- на данном шаге клиент предоставит область аутентификации (как правило, описание компьютера или системы, осуществляющей доступ) пользователю и запросит имя пользователя и пароль, в этот момент пользователь может принять решение об отмене;
- как только имя пользователя и пароль были предоставлены, клиент повторно посылает тот же самый запрос, но добавляет заголовок аутентификации, который включает код ответа;
- сервер принимает аутентификацию, и страница возвращается, а в случае, если имя пользователя является недействительным и/или пароль неверный, сервер может вернуть код ответа «401» — и клиент будет запрашивать их у пользователя еще раз [12].
- Digest-аутентификация обладает существенными недостатками:
- Digest-авторизация является медленной, так как необходимо выполнить два запроса;
- уязвима к атаке «человек посередине» (англ. man-in-the-middle), атака на воспроизведение;
- пароль, хранящийся на сервере, может быть взломан.

OAuth (oAuth2)

Принцип работы oAuth заключается в использовании временных токенов.

Схема действия оправдывает свое использование для клиентов третьей стороны: у них нет логина, пароля и разрешений, аналогичных пользовательским, поэтому необходимо отдельно хранить все разрешения для независимых клиентов. Для этих целей разработчик получает ключ API (API key) — длинные уникальные строки, содержащие произвольный набор символов, по сути, заменяющие собой комбинацию username/password, — а пользователи разрешают доступ к подконтрольным им данным. Например, доступ на просмотр имени, почтового адреса и т.п. [12].

После выдачи разрешений третьей стороне ей выдается токен на доступ, по которому они получают доступ уже к пользовательским данным.

Недостатки:

- сложнее в реализации;
- является зависимым от состояния (аналогичен cookie — stateless);
- уязвим к атакам «человек посередине».

Аутентификация по cookie

В идеальном RESTful-сервисе контроль за состояниями полностью производится на стороне клиента. Для не-браузерных клиентов cookies сложны в обработке.

Сценарий использования данного подхода заключается в следующем:

- API смотрит на заголовок «Authorization», в случае не-браузерных клиентов именно туда будет помещена информация для авторизации;
- если такой заголовок отсутствует, то проверяется сессионная cookie для осуществления авторизации на стороне сервера.

Этот подход имеет следующие недостатки:

- не отвечает требованиям RESTful-сервиса в вопросе независимости от состояния;
- уязвима к атакам «человек посередине»;
- на стороне сервера каким-то образом нужно хранить сессионную ID, что противоречит REST-идеологии.

Аутентификация по токенам и SSO

Такой способ аутентификации чаще всего применяется при построении распределенных систем, использующих единый сервис для входа (SSO), где одно приложение, выступающее в качестве сервиса-поставщика (англ. service provider, SP), делегирует функцию аутентификации пользователей другому приложению – сервису-поставщику идентификационных услуг (англ. identity provider, identity assertion provider, IdP). Сервис-поставщик идентификационных услуг решает следующие основные задачи:

- предоставляет идентификаторы пользователей, взаимодействующих с системой;
- предоставляет подтверждение того факта, что такой идентификатор известен сервису-поставщику;
- в случае существования такой необходимости предоставляет иную информацию о пользователе, которая известна сервису-поставщику. Это может быть достигнуто с помощью модуля аутентификации.

Реализация этого способа заключается в том, что IdP-сервис предоставляет достоверные сведения о пользователе в виде токена, а SP-приложение использует этот токен для идентификации, аутентификации и авторизации пользователя.

Для данного способа аутентификации существует несколько стандартов, определяющих протокол взаимодействия между клиентами (активными и пассивными), IdP и SP-приложениями и формат поддерживаемых токенов. Среди наиболее популярных стандартов — OAuth, OpenID Connect, SAML и WS-Federation.

Сам токен обычно представляет собой структуру данных, которая содержит информацию о том, кто сгенерировал токен, кто может быть получателем токена, срок действия токена, набор сведений о самом пользователе (claims). Кроме того, токен дополнительно подписывается для предотвращения несанкционированных изменений и гарантий подлинности.

Процесс аутентификации в данном методе выглядит следующим образом:

- клиент аутентифицируется в identity provider одним из способов, специфичным для него (пароль, ключ доступа, сертификат, Kerberos, и т.д.);
- клиент просит identity provider предоставить ему токен для конкретного SP-приложения, а identity provider генерирует токен и отправляет его клиенту;
- клиент аутентифицируется в SP-приложении при помощи этого токена.

При аутентификации с помощью токена SP-приложение должно выполнить следующие проверки:

- токен был выдан доверенным identity provider приложением (проверка поля issuer);
- токен предназначается текущему SP-приложению (проверка поля audience);
- срок действия токена еще не истек (проверка поля expiration date);
- токен подлинный и не был изменен (проверка подписи).

В случае успешной проверки SP-приложение выполняет авторизацию запроса на основании данных о пользователе, содержащихся в токене [12].

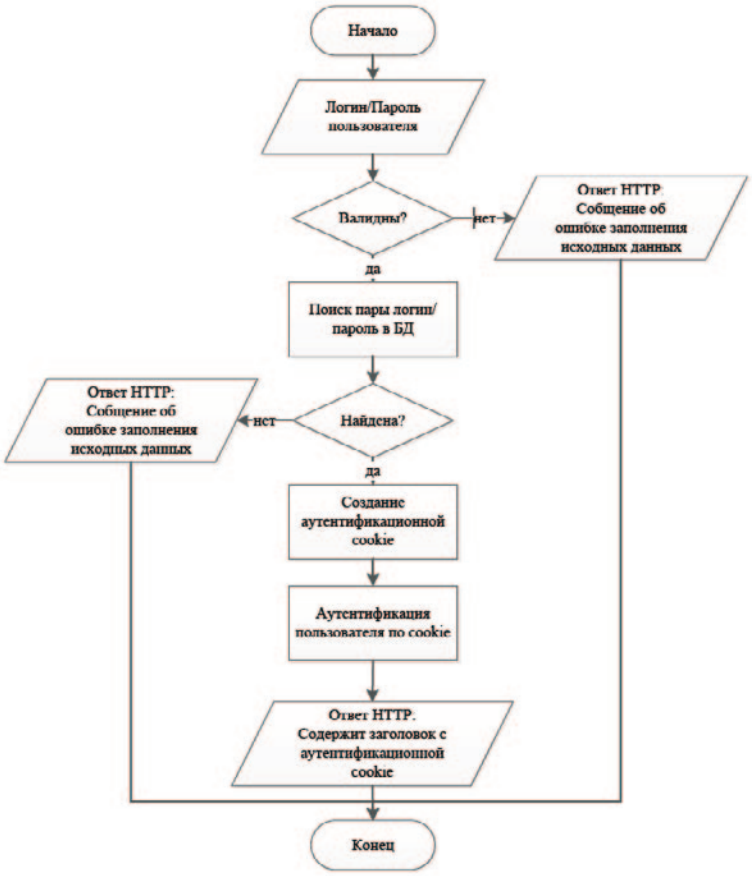


Рис. 1. Блок-схема алгоритма аутентификации пользователя по cookie.

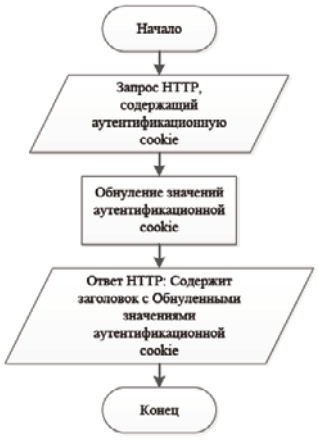


Рис. 2. Блок-схема алгоритма выхода из системы пользователя, авторизованного по cookie.

Обоснование выбора метода аутентификации

Выбор способа аутентификации определяется назначением API, а также основных типов клиентов, для которых предназначено данное API.

Назначением API может быть следующее:

- основное назначение: взаимодействие с front-end-частью системы для выполнения основной бизнес-логики системы;
- вторичное: использование методов, предоставляемых API, сторонними приложениями;
- точка доступа для осуществления однократного входа пользователя в рамках использования нескольких систем.

Основные типы клиентов можно подразделить на:

- браузерные;
- не-браузерные.
- Исходя из архитектуры разработанной системы [5], предлагается использовать следующие методы аутентификации:
- аутентификация по cookie, являющаяся классическим решением для браузеров;
- аутентификация по токену, являющаяся широко распространенным решением для RESTful-сервисов.

Реализация аутентификации и авторизации

Аутентификация по cookie

Для реализации метода входа в систему с дальнейшим присвоением пользователю аутентификационной cookie была выбрана стандартная реализация, имплементированная в OWIN Middleware.

Такой способ аутентификации требует предварительных настроек в конфигурационном файле, отвечающем за настройки аутентификации и авторизации проекта.

Для настройки аутентифицирующей cookie были выбраны следующие параметры:

- срок действия cookie – 12 часов с момента аутентификации;
- режим аутентификации – активный, что гарантирует создание пользовательской сущности, как только получен запрос.

Реализация аутентификации по cookie включает следующие два метода:

- POST api/account/session – вход в систему;
- DELETE api/account/session – выход из системы.

Блок-схемы алгоритмов аутентификации и выхода из учетной записи представлены на рисунках 1 и 2.

Аутентификация по токену

Авторизация на основе токенов состоит из нескольких компонентов:

- клиент, который обращается к веб-сервису — может представлять собой веб-браузер, мобильное приложение, десктопное приложение;
- веб-сервис, к ресурсу которого обращается клиент;
- токен доступа (access token), наличие которого дает доступ к ресурсам веб-сервиса;

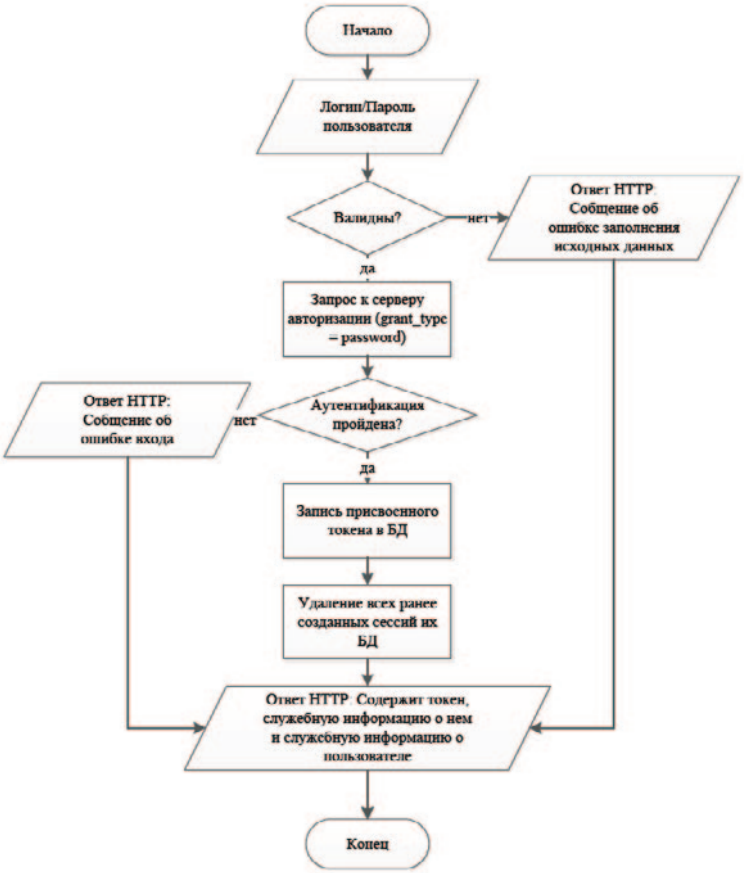


Рис. 3. Блок-схема алгоритма аутентификации пользователя по токену.

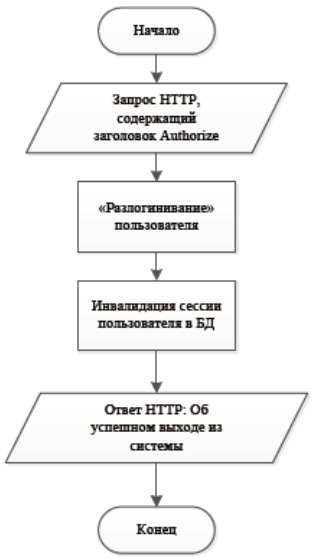


Рис. 4. Блок-схема алгоритма выхода пользователя по токену.

- bearer-токен — специальный вид токена доступа;
- сервер авторизации, который выдает токены доступа клиенту.

Реализация аутентификации по токену включает следующие два метода:

- POST api/account/token – вход в систему;
- DELETE api/account/token – выход из системы.
- Блок-схемы алгоритмов аутентификации и выхода из учетной записи представлены на рисунках 3 и 4.

Настройки аутентификации по токену имеют следующие параметры:

- срок действия токена – 14 дней с момента аутентификации;
- режим аутентификации – пассивный.

Регистрация пользователя и управление паролем

Наряду с процедурой аутентификации и авторизации пользователя также был реализован метод регистрации пользователя и управления его паролем:

Регистрация — POST api/account/register.

Смена пароля авторизованного пользователя — PUT api/account/password.

Запрос токена для сброса пароля неавторизованным пользователем — DELETE api/account/password.

Сброс пароля по токену неавторизованным пользователем — POST api/account/password?token=<token>&email=<email>.

Заключение

Решение задачи проектирования и внедрения системы сквозной аутентификации не является новым. Внедрение такой системы – это распространенная и довольно популярная практика для распределенных систем. Тем не менее, проблема построения системы единого входа является специфической для каждого сервиса в отдельности и зависит от многих исходных условий, которые накладываются на интеграционное решение в связи со спецификой ее уже существующих компонентов.

Рассмотренный в статье подход может быть применен для реализации интегрированных систем на основе использования облачных сервисов.

Литература

[1] Аникейчик Н.Д., Кинжагулов И.Ю., Федоров А.В. Планирование и управление исследованиями и разработками. Методическое пособие. – СПб.: Университет ИТМО, 2016. – 192
[2] Налоговый кодекс Российской Федерации (часть вторая) от 05.08.2000 № 117-ФЗ (ред. от 18.03.2023) (с изм. и доп., вступ. в силу с 01.04.2023)
[3] Постановление правительства РФ от 24 декабря 2008 г. № 988 «Об утверждении перечня научных исследований и опытно-конструкторских разработок, расходы налогоплательщика на которые в соответствии с пунктом 7 статьи 262 части второй Налогового кодекса Российской Федерации включаются в состав прочих расходов в размере фактических затрат с коэффициентом 1,5» (с изменениями и дополнениями) // https://base.garant.ru/12164440/
[4] Отчет о научно-исследовательской работе. Структура и правила оформления // https://docs.cntd.ru/document/1200026224
[5] Decision Support System for scientific and technical expertise / Belov A. V, Bikbaev B. I., Gevondyan M. S., Levitan D. A., Panina I. Yu. // in Proceedings of the 2023 Conference of Russian Young Researches in Electrical and Electronic Engineering (ElConRus). IEEE, 2023, p.p. 188-193
[6] https://antiplagiat.ru/
[7] https://searchplatform.rospatent.gov.ru/
[8] Эффективная классификация текстов на естественном языке и определение тональности речи с использованием выбранных методов машинного / Плешакова Е.С., Гатауллин С.Т., Осипов А.В., Романова Е.В., Самбуров Н.С. // обучения // Вопросы безопасности. – 2022. – No 4. – С. 1 — 14. DOI: 10.25136/2409-7543.2022.4.38658
[9] Анализ методов машинного обучения на примере задачи многоклассовой классификации текста / М. В. Лаптев // Информатика: проблемы, методы, технологии. – 2022. – С. 1155-1163
[10] Cloud Computing: Concepts, Technology & Architecture Thomas Erl, Ricardo Puttini, Zaigham Mahmood, NY, Pearson, 2013, p. 346
[11] Технология Single Sign On: инструменты централизованной аутентификации для функциональной системы сервисов. / А.Ю. Демидова, А.В. Жуков // Инженерный вестник Дона, №3, 2020, http://ivdon.ru/ru/magazine/archive/N3y2020/6353
[12] Обзор способов и протоколов аутентификации в веб-приложениях // https://habrahabr.ru/company/dataart/blog/262817/

Об авторах:

Александр Владимирович Белов,
профессор, руководитель Департамента прикладной математики МИЭМ НИУ ВШЭ,
avbelov@hse.ru

Александр Александрович Антышев,
ведущий научный сотрудник ФКУ НПО «СТиС» МВД России,
a166aa@yandex.ru

Маргарита Саркисовна Гевондян,
начальник правового отдела N 1 Межрегиональной инспекции ФНС России по крупнейшим налогоплательщикам N 1,
m.gevondyan.r9977@tax.gov.ru

Европейский союз на пути к цифровому суверенитету?

Мадина Касенова, Елена Воронина

Импульсом для подготовки настоящей статьи стал тот факт, что в декабре 2020 Европейский союз (далее – Евросоюз или ЕС) анонсировал начало разработки интернет-инфраструктуры, базирующейся на публичном (общедоступном) «европейском» DNS-резолвере [1] (далее – Проект DNS4EU). Эта инфраструктура должна стать технологическим средством, призванным качественно улучшить кибербезопасность европейского сегмента Интернета, усилить защиту конфиденциальности данных всех физических/юридических лиц в Евросоюзе, включая правительственные учреждения государств-членов ЕС и официальные институциональные органы ЕС. Проект DNS4EU направлен на решение жизненно значимой задачи по созданию технологических параметров цифровой независимости Евросоюза и одновременно рассматривается в качестве составного элемента общей концепции ЕС, нацеленной на обеспечение «европейского цифрового суверенитета» (European digital sovereignty).

Название настоящей статьи сформулировано в вопросительной коннотации, а это с необходимостью требует рассмотрения собственно самого понятия «суверенитет» в его контекстной интерпретации. Поэтому попробуем прежде всего разобраться, что имеется в виду под этим понятием в нашей статье. [1]


Изображение от Freepik

Первоначально необходимо обратиться к самому понятию «суверенитет», которое, безусловно, выступает правовой реальностью и юридическим символом, имманентно связанными с личностью государства. В свою очередь, самостоятельность и целостно-единая социальная сущность государства отражается в политической организации его публичной власти (законодательная, исполнительная, судебная). В общеправовом смысле «суверенитет» означает осуществление монопольного и полного верховенства публичной власти государства в пределах его национальных территориальных границ («внутренний суверенитет»), а также независимость и самостоятельность действия государства в международных отношениях («внешний суверенитет»). Такой подход зиждется на общепризнанной «вестфальской системе национального суверенитета». Стремительное расширение цифровых технологий не только решающим образом обусловливает развитие практически всех сфер общественной жизни, но также объективирует усложнение применяемых социально-регуляторных механизмов, в том числе диверсифицирует подходы к применению и осмыслению содержания традиционных категорий (включая их производные), не говоря о новых возникающих понятиях, их значениях, терминологическом применении и т.д. С понятием «суверенитет» в реалиях современных национальных правопорядков государств широко применяются такие производные, как «суверенитет информационной сферы», «технологический суверенитет», «цифровой суверенитет», «информационный суверенитет», «суверенитет информационного пространства» и др. При этом обозначенные производные понятия адаптивно применимы в контексте как «внутреннего», так и «внешнего» суверенитета.

Следующий момент связан со способами и формами реализации «внешнего суверенитета» государства, что de facto и de jure конкретизируется, в частности, в добровольном участии государства в международных организациях. Такое участие, с одной стороны, не означает утрату государством атрибутов своего суверенитета и своей международной правосубъектности, с другой стороны, означает ту или иную меру добровольного ограничения суверенитета государства (свободы его действий) с одновременным предоставлением создаваемой международной организации качества функциональной правосубъектности. В отношении

Евросоюза следует отметить его принципиальное отличие от иных международных межправительственных организаций. Обусловлено это тем, что Евросоюз, будучи по своей природе региональной международной организацией интеграционного характера, одновременно обладает уникальным политико-правовым статусом. По сути Евросоюз является единственным межгосударственным и «надгосударственным» объединением федеративного типа с особой моделью «добровольного ограничения своего суверенитета» государствами-членами, где inter alia: функционирует наднациональная правовая система наряду с национальными правовыми системами; наднациональные общие институциональные органы обладают властными полномочиями по принятию решений (как императивной, так и рекомендательной силы); наднациональные судебные органы наделены правом принятия нормативно-обязывающих прецедентных решений в отношении общих наднациональных структур, должностных лиц и институтов ЕС и государств-членов.

Уникальность специфики политико-правового статуса стала основанием для появления разделяемого в правовой доктрине тезиса о том, что поскольку Евросоюз не является государством (per se), но представляет собой «нечто большее, чем традиционная международная межгосударственная организация» в силу обладания им признаков «субгосударственного образования» федеративного типа, постольку не целесообразно анализировать характер отношений в правопорядке Евросоюза с «позиций традиционного государственного суверенитета». Соответственно, несмотря на то, что самодостаточность суверенитета Евросоюза не тождественна суверенитету государства, тем не менее в отношении Евросоюза позволительно сделать вывод о правомерности контекстного использования понятий «суверенитет», равно как и его производных — «европейский цифровой суверенитет» (European digital sovereignty), «технологический суверенитет» (technological sovereignty) и др.

Начиная с первого десятилетия XXI века Евросоюз предпринимает организационные, нормативно-правовые, технологические и прочие меры, призванные обеспечить «независимость европейского интернет-пространства» для поддержания «европейского цифрового суверенитета». Полагаем, что в рассматриваемом аспекте немаловажное значение имеет обладание Евросоюзом объединенным национальным доменом верхнего уровня (ccTLD) – .eu, доступным любому лицу (физическому/юридическому), базирующемуся на территории ЕС [2]. Примечательно, что с 2014 года домен верхнего уровня .eu распространяется на Европейскую экономическую зону, функционирующую на основе Соглашения о Европейском экономическом пространстве (Agreement on the European Economic Area, EEA) [3], участниками которого являются ЕС, страны-члены ЕС и три государства, не входящие в ЕС, – Исландия, Лихтенштейн, Норвегия. В практическом аспекте это означает доступность для любых лиц (физических/юридических) в Исландии, Лихтенштейне и Норвегии регистрации доменных имен в доменной зоне .eu. Стоит также напомнить, что упомянутое Соглашение нацелено на обеспечение свободной торговли и экономической интеграции государств-участников в рамках Единого Европейского цифрового рынка (Single Digital Market) [4], а также предусматривает нормативное правило о возможности распространения сферы действия актов вторичного законодательства ЕС на государства-члены Европейской экономической зоны (EEA).

К концу второго десятилетия текущего века Евросоюз осознал последствия своей цифровой зависимости от иностранных (прежде всего американских) интернет-технологий, соответственно, дискурс цифровой независимости и суверенитета Евросоюза определяет акцентуация на достижение технологической независимости, возможность установления контроля за иностранными поставщиками в части соблюдения ими регулирующих законодательных актов ЕС, обеспечение и поддержка кибербезопасности европейских пользователей и т.д. Такой дискурс во многом объясняется тем фактом, что современный ландшафт Евросоюза в сфере телекоммуникаций преимущественно формируется и определяется доминирующей ролью американских технологических компаний-гигантов. Уместно в этой связи обратить внимание на справедливость тезиса ряда экспертов о том, что такое «доминирование» объективируется технологической спецификой базовой архитектуры Интернета [5]. Речь о том, что Интернет кардинально отличается от традиционных национальных коммуникационных сетей и обладает специфической технологической архитектурой, база которой позволяет интернет-компаниям (в первую очередь, американским технологическим компаниям) масштабировать сетевую инфраструктуру без учета национальных границ, формировать сервисные платформы услуг с трансграничным охватом всего диапазона сети. Доминирование американских (иностранных) интернет-компаний на европейском телекоммуникационном рынке не только не способствует развитию европейских компаний (мелкого и среднего бизнеса, стартапов и проч.), подрывает конкурентную среду в цифровом секторе, но и в целом негативно влияет на независимость европейского интернет-пространства.

Устранить «дискомфортные эффекты» доминирования американских (иностранных) компаний в цифровом пространстве Евросоюза призваны принятые в «пакетном» варианте (и вступившие в силу) два регламента Европейского парламента и Совета: «Регламент (ЕС) 2022/1925 о цифровых рынках» (Digital Markets Act, DMA) и «Регламент (ЕС) 2022/2065 о цифровых услугах» (Digital Services Act, DSA). Названные регламенты содержат концептуальные подходы ЕС, касающиеся политики, правил и порядка регулирования функционирования онлайн-платформ как значимого структурного элемента единого европейского цифрового рынка [6]. Отметим, что в содержательном плане названные регламенты – DMA и DSA – подробно проанализированы в декабрьском номере журнала «Интернет изнутри» [7].

Дискурс цифровой независимости рассматривается в Евросоюзе в т.ч. с точки зрения создания защитных технологических инструментов, чему призван содействовать Проект DNS4EU, реализация которого рассчитана на трехлетний период (2023-2026 гг.). Проект DNS4EU должен выступить альтернативой нынешним публичным (общедоступным) DNS-резолверам, которые предоставляются американскими технологическими гигантами. Евросоюз намерен сделать данный DNS-резолвер в качестве официально рекомендованного для государственных и правительственных учреждений в масштабе европейского континента. Планируется,


Изображение от Freepik

что технология DNS4EU позволит обеспечить лиц Евросоюза (физических/юридических) как бесплатными DNS-услугами, так и услугами повышенной безопасности премиум-класса, сохраняя при этом высокие стандарты конфиденциальность данных лиц в ЕС, включая хранение данных пользователей в цифровом пространстве Евросоюза [8].

На момент написания настоящей статьи даже первый (начальный) этап Проекта DNS4EU окончательно не завершен, поэтому рассмотреть саму сущность разрабатываемой технологии DNS4EU не представляется возможным. В настоящее время целый ряд вопросов технического и организационного порядка по Проекту DNS4EU остаются открытыми либо находятся в процессе обсуждения. Широта, критичность и плюрализм мнений, высказываемых стейкхолдерами на многих европейских площадках, затрагивают такие вопросы, как параметры развертывания оборудования всей сети DNS4EU в Европе, включая определение центров обработки данных по всей Европе; функциональность публичных/общедоступных DNS-резолверов (public resolvers) в части контроля над трафиком как с точки зрения безопасности, так и с точки зрения фильтрации контента, родительского контроля, блокировки рекламы и т. д.; варианты измерения эффективности системы DNS4EU (включая оптимальную бизнес-модель монетизации и решение вопросов государственных субвенций) и т.д. [9]

Принимая во внимание специфику институционального механизма функционирования ЕС (включая разность объема компетенций руководящих органов ЕС), в качестве центрального органа по Проекту DNS4EU была определена Европейская Комиссия (далее – Еврокомиссия) [10]. Еврокомиссия приняла решение предоставить организационно-финансовую помощь в создании международного общеевропейского консорциума (далее – EU-Консорциум) с тем, чтобы каждый пользователь Евросоюза мог получить доступ к технологии DNS4EU. Определить однозначно правовой статус EU-Консорциума непросто. Формально-юридически в структурный состав EU-Консорциума входят 13 членов из 10 стран-членов Евросоюза, а деятельность EU-Консорциума возглавляется чешской компанией Whalebone, которая аккумулирует всю информацию по Проекту DNS4EU [11]. Вместе с тем деятельность EU-Консорциума опирается на организационную модель, охватывающую широкий круг лиц европейского сектора телекоммуникаций и технологий: интернет-компании частного сектора (операторы интернет-технологий/интернет-услуг и т.д.), научно-исследовательские институты, образовательные сети (NREN) НПО, государственные учреждения стран-членов ЕС, отраслевые и национальные группы реагирования на компьютерные чрезвычайные ситуации (CERT), национальные исследовательские и образовательные сети (NREN), независимых экспертов по кибербезопасности ряда стран-членов ЕС. Названные лица участвуют в деятельности EU-Консорциума либо в качестве членов, либо как ассоциированные партнеры [12]. Из этого можно сделать вывод, что EU-Консорциум не обладает правосубъектностью, т.е. не может рассматриваться в качестве юридического лица конкретного государства-члена ЕС, а также не может относиться к институциональным органам ЕС. Несмотря на это обстоятельство, деятельность EU-Консорциума не выпадает из сферы действия национальных регулирующих органов, равно как и не оказывается вне нормативных правил институциональных органов Евросоюза. В этой связи, как минимум, следует принять во внимание, что чешская компания Whalebone является «главой» и организационным «ядром» EU-Консорциума, и свою деятельность EU-Консорциум осуществляет также из Чехии, а это в практическом плане означает обязательность соблюдения EU-Консорциумом соответствующих нормативных правил и положений правопорядка Чехии.

С учетом указанного ранее трехлетнего периода реализации Проекта DNS4EU, предметная и функциональная компетенции EU-Консорциума конкретизированы и комплексно сосредоточены на а) разработке и внедрении собственно самой интернет-инфраструктуры технологии DNS4EU для создания общеевропейской защитной DNS-службы; б) обеспечении подключения к публичным (общедоступным) DNS-резолверам


Изображение от Freepik

100 миллионов пользователей ЕС; в) объединении существующей инфраструктуры телекоммуникационного оператора и интернет-провайдера с новыми публичными (общедоступными) DNS-резолверами [13]. После запланированного завершения Проекта DNS4EU и полного развертывания технологии DNS4EU (2026 г.) EU-Консорциум рассматривается в качестве организации, призванной осуществлять последующее управление использованием системой DNS4EU в рамках Евросоюза, поэтому EU-Консорциум создан на неопределенный срок.

***

Вынесенный в название настоящей статьи вопрос не является риторическим в силу нацеленности Европейского союза идти по пути обеспечения независимости своего интернет-пространства и поддержания функциональной целостности европейской цифровой сферы в технологическом и организационном плане. В общем плане положительно отвечая на заданный вопрос, надлежит принять во внимание ряд взаимосвязанных вопросов, получив ответы на которые, можно адекватно обсуждать средства, формы и методы реализации цифрового суверенитета Евросоюза. Это тем более важно в силу того, что цифровую зависимость Евросоюза еще предстоит преодолеть, равно как предстоит обеспечить цифровой суверенитет Евросоюза посредством подключения его общих институциональных механизмов. Рассмотренные в формате статьи положения отнюдь не отражают всей палитры концептуальных подходов Евросоюза к решению поставленной задачи. Регуляторные инициативы в цифровом секторе носят характер новаций и поэтому требуют постоянной «тонкой настройки» для исключения негативного влияния на профильные рынки без ущерба идеям безопасности, а потому «Продолжение следует».

Литература:

[1] European Public DNS Resolver. URL: https://www.ripe.net/participate/meetings/open-house/ripe-ncc-open-house-dns4eu
[2] Основополагающие документы домена верхнего уровня «.eu»: Регламент Европейского парламента и Совета ЕС от 22 апреля 2002 г. N 733/2002. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32002R0733; Регламент Комиссии ЕС от 28 апреля 2004 г. N 874/2004. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32004R0874
[3] Agreement on the European Economic Area, EEA, именуемое также Соглашением об Европейской экономической Зоной, от 01.01.1994 г. URL:https://www.efta.int/eea/eea-agreement#:~:text=The%20Agreement%20on%20the%20European,as%20the%20%22Internal%20Market%22
[4] Single Digital Market. URL: https://ec.europa.eu/eurostat/cache/infographs/ict/bloc-4.html; см. также например, Wahdani F., Alfauri M. .eu Top Level Domain Name & Free Movement of Services: the EU Policy Over Single Digitsl Market. URL: https://seaopenresearch.eu/Journals/articles/CMJ2020_I1_7.pdf
[5] См. например, Huston G. Some Thoughts on DNS4EU – the European Commission's Intention to Support the Development of a New European DNS Resolver. URL: https://circleid.com/posts/20220213-some-thoughts-on-dns4eu-new-european-dns-resolver
[6] Об этом подробнее, например: Chiarella Maria Luisa. Digital Markets Act (DMA) and Digital Services Act (DSA): New Rules for the EU Digital Environment. URL: https://www.athensjournals.gr/law/2023-9-1-2-Chiarella.pdf
[7] Журнал «Интернет изнутри» № 16 (декабрь 2021). С. 34-41
[8] URL:https://ripe86.ripe.net/wp-content/uploads/presentations/112-ripe86-dns-resolver-tf.pdf; а также URL:https://fel.cvut.cz/en/what-s-on/news/31370-the-european-commission-plans-to-onboard-100-million-people-to-a-new-eu-based-dns-internet-infrastructure-the-dns4eu-will-be-developed-by-international-consortium-including-ai-center-fee-ctu
[9] См, например, Huston G. Measuring Open Resolver Use in EU. URL: https://ripe86.ripe.net/wp-content/uploads/presentations/115-2023-05-25-dns4eu.pdf; информацию о целевой группе DNS-Resolver. URL:https://ripe86.ripe.net/wp-content/uploads/presentations/112-ripe86-dns-resolver-tf.pdf
[10] О статусе Европейской комиссии см. подробнее, например, «Договор о Европейском Союзе», «Договор о функционировании Европейского Союза». СПС КонсультантПлюс
[11] https://www.whalebone.io/dns4eu
[12] Состав EU-Консорциум de facto объединяет представителей от всех групп стейкхолдеров телекоммуникационного сектора ЕС. URL: https://www.whalebone.io/post/press-release-dns4eu
[13] Kyriakou A. Shielding Europe – DNS4EU's Pan-European Protective DNS Service. https://ripe86.ripe.net/wp-content/uploads/presentations/118-Shielding-Europe-DNS4EU.pdf

Об авторах:

Мадина Балташевна Касенова, доктор юридических наук, профессор кафедры теории и истории частного права ФГБН «Исследовательский центр частного права имени С.С. Алексеева при Президенте РФ», mbk.07@mail.ru

Елена Павловна Воронина, директор по развитию Фонда развития сетевых технологий «ИнДата», elin@indata.org.ru

Новости науки и техники

Рынок облачной инфраструктуры превысил объем в 120 миллиардов долларов

Аналитическая компания Gartner представила результаты своего исследования рынка облачной инфраструктуры (infrastructure-as-a-service, IaaS). Согласно его данным, темпы роста в прошлом году составили 29,7%. Это позволило рынку достичь объема в 120,3 миллиарда долларов. Годом ранее объем этого рынка оценивался в 92,8 миллиарда долларов. Тем не менее, темпы роста предыдущего года были выше – на уровне 40%. Эксперты объясняют это тем, что во второй половине 2022 года бизнес активно стремился к сокращению расходов и более эффективному использованию имеющихся облачных ресурсов. Вице-президент Gartner Сид Нэг (Sid Nag) полагает, что эта же тенденция сохранится и в текущем году и может считаться показателем зрелости рынка. В то же время он уверен, что потенциал роста все еще очень велик, и ожидает активизации уже в 2024 году.

Лидерами рынка являются компании Amazon со своим сервисом Amazon Web Services (AWS) и Microsoft с платформой Azure. Их доли рынка составляют 40% и 21,5% соответственно. В долларовом эквиваленте это 48 и 26 миллиардов долларов. Таким образом, на долю двух этих гигантов приходится почти две трети всего рынка облачной инфраструктуры. Третьей с большим отрывом от лидеров идет китайская компания Alibaba, чья доля рынка оценивается в 9,28 миллиарда долларов. Буквально в затылок ей дышит Google – 9 миллиардов долларов. И замыкает первую пятерку Huawei – 5,25 миллиарда долларов.

При этом Alibaba полностью доминирует на китайском рынке, однако потенциал выходы за его пределы выглядит весьма проблематичным, что сдерживает рост. Отчасти по этой причине облачный бизнес Alibaba был выделен в самостоятельную структуру. Корпорация Google, напротив, продемонстрировала в минувшем году лучшие показатели роста во всей первой пятерке – 41%. Это объясняется как щедрыми инвестициями в собственные облачные решения, так и расширением партнерских программ.

В этой связи уместно привести и данные другого исследования, выполненного компанией Synergy Research Group. Оно показывает, что 10 лет назад крупные технологические компании тратили более 80 миллиардов долларов на аппаратное и программное обеспечение своих дата-центров и лишь менее 10 миллиардов долларов на сервисы облачной инфраструктуры. Сегодня расходы на аппаратное и программное обеспечение дата-центров растут со среднегодовыми темпами порядка 2%. А среднегодовые темпы роста расходов на облачные сервисы составляют 42%.

Источник: The Register
https://www.theregister.com/2023/07/18/aws_azure_cloud_market/

Изображение от Freepik

Компания NexGen Cloud создает «супероблако» для европейских проектов искусственного интеллекта

Британская компания NexGen Cloud, предоставляющая услуги облачной инфраструктуры в качестве сервиса, объявила об амбициозном проекте. Она инвестирует 1 миллиард долларов в создание одной из первых в Европе облачных платформ для разработок в области искусственного интеллекта. В законченном виде платформа AI Supercloud объединит 20 тысяч ускорителей с тензорными ядрами H100 Tensor Core от NVIDIA, элитным членом партнерской сети которой NexGen Cloud является.

Компания уже оформила заказы на аппаратное и программное обеспечение на 576 миллионов долларов. «Искусственный интеллект должен принести успех нациям и процветание гражданам. Проект AI Supercloud позволит бизнесу в полной мере воспользоваться преимуществами нового витка эволюции технологий, оставаясь при этом в европейской юрисдикции с гарантированными ею суверенитетом и безопасностью данных», — заявил глава NexGen Cloud Крис Старки (Christopher Starkey). Вычислительные мощности проекта будут доступны европейским компаниям, организациям и правительственным учреждениям для выполнения ресурсоемких задач, связанных с исследованиями и разработками в области искусственного интеллекта.

Проект реализуется за счет финансового партнерства с инвестиционной компанией Moore and Moore Investments Group (MMI). Специально для него создан фонд, который привлекает средства частных инвесторов. Предполагается, что AI Supercloud начнет работать в полном объеме летом будущего года.

Источник: CloudTech
https://www.cloudcomputing-news.net/news/2023/oct/10/nexgen-clouds-1bn-ai-supercloud-to-turbocharge-ai-in-europe/

Генеративный искусственный интеллект и миграция в облако

В последнее время появляется все большее число публикаций, посвященных возможности использовать генеративные модели искусственного интеллекта для миграции в облако – переноса приложений и данных крупных компаний с собственных локальных серверов на серверы общедоступных облачных служб. Миграция в облако позволяет сократить расходы на IT-инфраструктуру и повысить производительность. Однако сам процесс миграции сопряжен с серьезными сложностями и чреват рисками. Свою точку зрения на этот вопрос ресурсу InfoWorld высказал Дэвид Линтикам (David Linthicum) – ученый и консультант, признанный эксперт в сфере облачных технологий, автор 15 книг, последняя из которых посвящена именно облачным вычислениям (An Insider's Guide to Cloud Computing). Линтикам организовывал и принимал активное участие во многих миграциях, и его мнение представляется весьма ценным.

Дэвид Линтикам подчеркивает, что любая миграция в облако несет риски нарушения бизнес-процессов компании, потери либо утечки данных и создает угрозы безопасности. Чаще всего подобные инциденты возникают, когда компания использует стратегию простого, механического перемещения (lift and shift). Ее кажущееся преимущество состоит в простоте и дешевизне. Однако в реальности за последствия ошибок при такой миграции приходится расплачиваться очень дорого.

Первым этапом миграции должен быть тщательнейший анализ: текущее состояние кодов и баз данных, механизмы интеграции, способы управления и обеспечения безопасности – все это и многое другое должно пройти своего рода инвентаризацию. Компании зачастую пренебрегают этим этапом даже не потому, что они о нем не знают, а потому что эта работа является чрезвычайно длительной и кропотливой, требующей серьезных ресурсов и затрат. И возможность переложить ее на плечи генеративного искусственного интеллекта видится Линтикаму хорошим решением. Искусственный интеллект способен осуществить анализ всех перечисленных аспектов и составить поэтапный план миграции, указать на слабости в защите, порекомендовать ту или иную стратегию, основываясь на объеме и степени конфиденциальности данных и пропускных способностях сетей. Он также может подобрать наиболее подходящего облачного провайдера, основываясь на потребностях компании.

Резюмируя, Дэвид Линтикам иронически замечает, что генеративный искусственный интеллект уравнивает шансы на успешную миграцию в облако для компаний, которые готовы упорно трудиться, готовя такую миграцию, и для «ленивых компаний», которым подготовительный этап представляется слишком сложным.

Источник: Info World
https://www.infoworld.com/article/3708728/generative-ai-and-migrations-to-the-public-cloud.html

Хакеры атаковали облачные сервисы Microsoft

Корпорация Microsoft признала, что подверглась DDoS-атакам: 7, 8 и 9 июня были последовательно атакованы облачные сервисы Outlook, OneDrive и Azure. В результате доступа к сервисам временно лишились миллионы пользователей. На тот момент представители Microsoft ограничились лишь констатацией «технических проблем», но позже подтвердили, что причиной сбоев стали масштабные DDoS-атаки.

В сообщении корпорации сказано, что организаторы атаки располагают значительными ресурсами и возможностями. Они использовали большое число виртуальных выделенных серверов, арендованную облачную инфраструктуру и открытые прокси. В результате им удалось достичь объемов трафика, временно превысивших возможности облачных сервисов Microsoft. В настоящее время компания ведет детальное расследование инцидента и усиливает защиту своей инфраструктуры. Она подчеркивает, что нет никаких свидетельств того, что атакующие могли получить доступ к данным пользователей или скомпрометировать их.

Группировка, стоящая за атаками, идентифицирована в сообщении Microsoft как Storm-1359. Но она более известна под названием Anonymous Sudan. Эта хакерская группа заявила о себе в начале нынешнего года, а в заголовках новостей появилась после серии атак на IT-инфраструктуру скандинавской авиакомпании Scandinavian Airlines (SAS). Поводом для них послужило сожжение Корана в ходе одной из политических акций в Стокгольме. Теперь хакеры грозят карой всем, кто проявит себя недружественным образом в отношении Судана и ислама. Так, атака на Microsoft объяснена тем, что власти США якобы оказывают давление на страну и даже угрожают ввести туда свои войска. Впрочем, о материальных интересах хакеры Anonymous Sudan тоже не забывают. Они сообщили в социальных сетях, что готовы научить специалистов Microsoft отражать масштабные DDoS-атаки и прекратить свои нападения за 1 миллион долларов.

Источник: Bleeping computer
https://www.bleepingcomputer.com/news/microsoft/microsoft-confirms-azure-outlook-outages-caused-by-ddos-attacks/


Изображение от Freepik

Новости доменной индустрии

Сентябрь 2023: домен .ru сохранил лидерство

По данным «Технического центра Интернет», в сентябре 2023 года российская зона .ru выросла на рекордные 48 453 домена и сохранила первое место по темпам роста среди национальных доменов!

Кириллическая зона .рф в сентябре также выросла на 3940 доменов (+0,56%).

Кроме России наибольший рост в сентябре показали национальные зоны Германии .de (22 432 домена) и Бразилии .br (+19 973 домена).

Среди общих доменов традиционно наибольший рост у зоны .com – она прибавила 2 817 114 доменов, а среди новых доменов – .top (+226 309 доменов) и .online (+181 352 домена).

Источник: https://d-russia.ru/statistika-domennyh-imjon-sentjabr-2023.html

Closed generics остаются под запретом

Как сообщает Domain Insite, делегирование Closed generics, вероятнее всего, останется под запретом и на втором этапе программы New gTLD.

Это стало понятно после того, как рабочая группа ICANN, в задачи которой входила выработка политик в отношении этих доменов, фактически признала свою неспособность достичь результата.

Closed generics – домены верхнего уровня, совпадающие с общеупотребимыми словами (.music, .car, .baby, .cloud, .burger и т.д.), но не являющиеся товарными знаками. При этом регистратуры намеревались использовать их как домены-бренды: закрыв возможность сторонних регистраций.

На первом этапе запуска New gTLD ICANN не возражала против их делегирования, и число заявок на них превысило 180. Однако категорически против Closed generics выступил Правительственный консультативный комитет (GAC), и их делегирование было отложено.

Но в ходе подготовки второго этапа New gTLD проблема вновь вышла на первый план. И после длительных обсуждений и переговоров руководители рабочей группы опубликовали письмо, в котором объявили о том, что «не видят необходимости увязывать решение вопроса о Closed generics с началом следующего этапа программы New gTLD». И это означает, что решения этого вопроса в ближайшее время не предвидится.

Источник: https://domainincite.com/28986-closed-generics-ban-likely-to-remain-after-another-policy-group-failure

New gTLD набирают обороты

На фоне снижения числа регистраций в домене .com и стагнации в зонах .net и .org многие new gTLD демонстрируют впечатляющий рост.

По данным Координационного центра доменов .RU/.РФ, по итогам III квартала 2023 года:

- .online выросла на 13,9%;
- .top выросла на 18,7%;
- .shop выросла на 11,6%;
- .site выросла на 8,5%;
- .store выросла на 11,6%.

Интересно, что эти зоны продолжают расти не первый квартал. Так, с начала 2023 года .online выросла на 768,5 тысячи доменов, .top – на 741 тысячу доменов, .shop – 559,8 тысячи доменов, а .site – 331,5 тысячи доменов.

Источник: https://cctld.ru/upload/iblock/f62/awvi5ao3rkn8vhkielmcbpg4w6pjjg70/World_stat_2023_3kv_.pdf

Регистратура Public Interest Registry предоставила Красному Кресту право требовать блокировку доменных имен

Регистратура Public Interest Registry (PIR) объявила о заключении соглашения с Американским обществом Красного Креста. Соглашение наделяет Красный Крест статусом «доверенного уведомителя» (trusted notifier). Это означает, что организация может напрямую обращаться к регистратуре с требованием блокировки доменных имен. Практика trusted notifier достаточно распространена среди регистратур, но обычно этот статус предоставляется крупным правообладателям, а также организациям, ведущим борьбу с распространением детской порнографии. Его предоставление Красному Кресту – первый случай подобного рода.

Ресурс Domain Incite, сообщая эту новость, отмечает, что статус trusted notifier предоставляет право Красному Кресту требовать лишь блокировки доменов, используемых именно для мошеннических сайтов. Критика или сатира – в том числе и по адресу Красного Креста – не могут рассматриваться как основание для требования блокировки. Соглашение распространяется на все доменные зоны под управ-

лением регистратуры PIR. Прежде всего, это, конечно, домен .org, но вмешательство Красного Креста может быть актуально и для доменных зон .charity и .giving, непосредственно связанных с темой благотворительности.

Источник: https://domainincite.com/28835-red-cross-gets-takedown-powers-over-org-domains

Компания Verisign запустила сайт DNIB.com

Компания Verisign объявила о запуске веб-сайта DNIB.com. Имя домена является аббревиатурой от Domain Name Industry Brief – ежеквартального отчета Verisign, который является одним из самых влиятельных и авторитетных источников информации о состоянии доменной индустрии. Именно на сайте DNIB теперь и будут публиковаться отчеты Verisign. Но только ими контент сайта, разумеется, не ограничится. Анонс обещает постоянно обновляемы информационные и аналитические материалы по вопросам технологий, проблем управления Интернетом, доменного бизнеса и т.д.

Помимо этого, ресурс предлагает возможность быстрого поиска интересующих публикаций по тэгам и несколько информационных панелей, позволяющих ежедневно отслеживать динамику ряда ключевых статистических параметров. Есть все основания полагать, что сайт DNIB.com станет ценным источником информации как для профессионалов доменной индустрии и доменного бизнеса, так и для тех, кто стремится больше узнать о состоянии и функционировании системы DNS.

Источник: https://blog.verisign.com/domain-names/announcing-launch-dnib-website/

Блокчейн-стартап будет участвовать в следующем этапе программы новых доменов

Зарегистрированный в Лас-Вегасе стартап D3 Global объявил о том, что привлек 5 миллионов долларов на начальном этапе финансирования. Средства будут направлены на участие в следующем этапе программы новых общих доменов верхнего уровня, который может стартовать, предположительно, в 2025 году. Руководителем D3 Global является предприниматель Фред Хсю (Fred Hsu), создавший в свое время сервис Oversee.net. Также в число основателей стартапа входят Пол Стахура (Paul Stahura), один из создателей Donuts (ныне Identity Digital) и Шайан Ростам (Shayan Rostam), входивший в руководство Uniregistry. Все они имеют огромный опыт весьма успешной работы в доменной индустрии, а потому их нынешняя инициатива, безусловно, заслуживает внимания, констатирует ресурс Domain Incite, сообщая эту новость.

Чрезвычайно примечательно, что новая компания декларирует своей целью «преодоление пропасти между традиционными и блокчейн-доменами». Она намерена подавать заявки на право управления традиционными новыми общими доменами верхнего уровня и «обеспечивать их взаимодействие с доменными системами, использующими технологию блокчейн». Каким именно образом будет обеспечиваться это взаимодействие, в настоящий момент неизвестно. Помимо этого, в планы компании входит создание торговой площадки как для традиционных, так и для блокчейн-доменов. Предполагается, что использование блокчейн-технологий позволит заметно повысить прозрачность операций, отсутствие которой является общепризнанным слабым местом большинства подобных площадок. Учитывая, мягко говоря, настороженное отношение корпорации ICANN к блокчейн-доменам, будет весьма интересно узнать, как сложится судьба D3 Global.

Источник: https://domainincite.com/29040-blockchain-startup-gets-5-million-to-apply-for-gtlds

CENTR опубликовал отчет о развитии европейских доменов

Ассоциация европейских национальных регистратур (CENTR) опубликовала отчет о состоянии и тенденциях развития доменного рынка в I полугодии 2023 года.

Что в нем интересного?

Медианный рост европейских национальных доменов составил 2%. И это хороший результат, особенно учитывая низкие показатели национальных доменов в начале года. При этом рост российских зон .ru и .рф в I полугодии 2023 года составил 2% и 3,1% соответственно.

Средний процент продления регистраций национальных доменов при этом снизился и составил 80,8%, а медианный коэффициент спроса составил 1,2.

Средняя стоимость регистрации новых доменов выросла и достигла 10,3 евро, в то время как год назад она составляла 9,9 евро. В российских зонах стоимость регистрации остается самой низкой в Европе и в среднем составляет 1,2-2 евро (119-199 рублей в зависимости от компании-регистратора).

43% доменов в европейских национальных зонах имеют работающий веб-сайт. Для сравнения, в российских зонах .ru и .рф этот показатель составляет 63,5% и 60% соответственно.

Источник: https://stats.centr.org/stats/global

MSK IX

DNS

DNS-RESOLVER MSK-IX для ISP

Получите быстрый и безопасный доступ к информационным ресурсам сети Интернет

Скорость
Максимально быстрый ответ на DNS-запрос за счёт использования технологии Anycast

Надёжный
Обеспечивает доступность сервиса на уровне выше 99,98%

Высокопроизводительный
Обрабатывает 200 000+ (UDP) запросов в секунду

Безопасный
Поддерживает протоколы безопасности: DNSSEC, DoT, DoH

ANYCAST DNS

Удобный и эффективный сервис по размещению DNS-зон на нескольких DNS-узлах, использующих единую IP адресацию.

Скорость – максимально быстрый ответ на DNS-запрос за счёт использования технологии Anycast

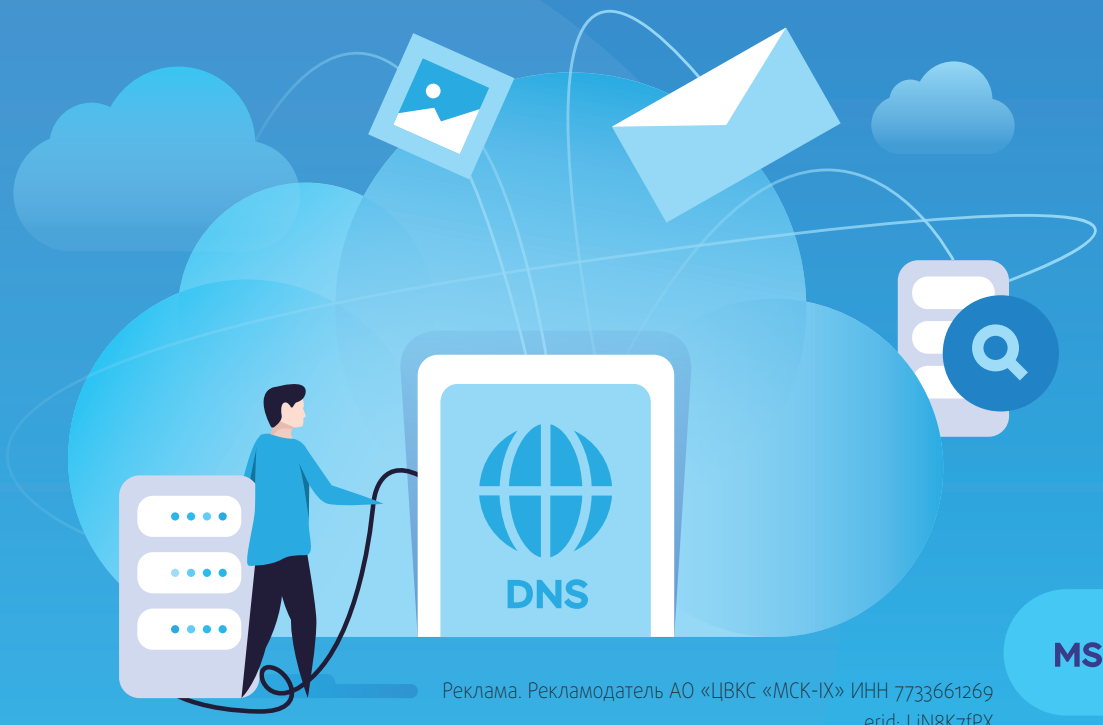
Безопасность – поддержка DNSSEC как средства минимизации атак, связанных с подменой IP-адреса

Надёжность – работоспособность сервиса не зависит от работоспособности отдельного узла Anycast

Технологичность – постоянный мониторинг оказываемых услуг и оборудования, а также техническая поддержка заказчиков

Удобство – редактор DNS-зон с массовым созданием списка зон для списка доменов и загрузкой из внешних источников

Статусность - возможность именования сервиса DNS собственными доменными именами (white-label)



MSK-IX.RU

Интернет изнутри