05.13.18

ОТКАЗОУСТОЙЧИВОСТЬ И БЕЗОПАСНОСТЬ ДОСТУПА В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

Х.Х. Судани[1], М.Б. Абросимов[2]

[1]*Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского, Министерство науки и технологий Ирака, Багдад, Ирак*

[2] *Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского, Саратов*

Аннотация: Рассмотрены ключевые вопросы, связанные с организацией инфраструктуры облачных технологий. Описаны основные виды «облаков» и принципы организации их работы, показаны основные подходы к обеспечению отказоустойчивости облачных систем, в том числе особенности методов восстановления системы после отказов на основе сохранения состояний процессов. Сформулирован вопрос комплексной оценки надёжности инфраструктуры облачных вычислений, указаны основные проблемы и достоинства «облачных вычислений».

Достигнутые результаты: описаны основные аспекты функционирования поставщиков и потребителей услуг облачных вычислений, показаны особенности их взаимоотношений и системный характер вопроса. Сформулирована задача комплексной оценки надёжности соответствующей инфраструктуры.

Ключевые слова: *инфраструктура, облачные вычисления, центры обработки данных, отказоустойчивость, надёжность*

На сегодняшний день большое распространение получила модель обеспечения сетевого доступа пользователей к общему фонду вычислительных ресурсов, для обозначения которой условимся использовать общеупотребимый в настоящее время термин «облачные вычисления».

Облачные вычисления (ОВ) – это технология, которая предоставляет удалённый доступ к аппаратному и программному обеспечению через Интернет либо локальную сеть [1]. Создание инфраструктуры ОВ предполагает развёртывание совокупности определённым образом связанных центров обработки данных (ЦОД), при этом в общем случае конечный потребитель технологии не имеет возможности отличить физически обособленные ресурсы ЦОД от виртуальных. Такая особенность ОВ обеспечивает пользователю возможность использования удаленных ресурсов, не задумываясь о технологических аспектах их функционирования, что исключает из рассмотрения одну из составляющих сложности организации вычислительного процесса (более строго: переносит данную составляющую задачи на сторону поставщика услуги ОВ). Таким образом, в бытовом смысле под ОВ можно понимать единую схему доступа пользователя к вычислительным ресурсам поставщика.

Концепция ОВ берёт своё начало ещё в конце 50-х годов XX века [4, 3], однако лишь развитие информационных технологий обеспечило возможность её практического воплощения. Современное же состояние ИТ, а также прогнозируемое на ближайшее будущее её развитие, позволяют рассматривать ОВ в качестве технологии стратегического характера.

Работа при использовании ОВ строится следующим образом [1]:

1. Первый этап: аренда пользователем удалённого ресурса (сервера) у какой-либо из предоставляющих данную услугу организаций (Amazon AWS [9], Google Cloud [7], Microsoft Azure [10], российская бизнес-площадка «IT-Град» [8] и т. п.);
2. Второй этап: загрузка пользователем потребной для решения его задач конфигурации программного обеспечения (ПО) на арендованный сервер;
3. Третий этап: собственно жизненный цикл загруженного ПО.

Как правило, в инфраструктуре ОВ предусмотрена возможность самоуправления и делегирования полномочий для организации защищённого доступа к вычислительным ресурсам всех участников виртуальной работы. Перечислим (согласно [1]) основные выделяемые роли участников:

1. Cloudprovider (продавец облачных услуг);
2. Cloud consumer (пользователь услуг);
3. Cloud broker (посредник между облачными провайдерами и потребителями, управляющий производительностью);
4. Cloud carrier (посредник между облачными провайдерами и потребителями, предоставляющий услуги подключения и транспорт данных);
5. Cloud auditor (компания или физическое лицо, выполняющие независимую оценку облачных услуг).

В общем случае ряд участников может исполнять более одной из перечисленных ролей (характерно для поставщиков услуги ОВ, которые одновременно являются поставщиками услуг связи). В то же время, возможна и ситуация, когда, например, роль аудитора остаётся не занятой.

В течение жизненного цикла ПО пользователь имеет механизмы управления (запрос дополнительных и освобождения лишних на текущий момент ресурсов, подключение дополнительных средств безопасности, изменение конфигурации и прочее) арендованными серверами через Интернет. Очевидно, что такие механизмы уступают в гибкости в сравнении с локально размещёнными ресурсами, но на практике различие существенным не является. Ключевой же особенностью данной схемы для пользователя является необходимость оплачивать только фактическое использование для хранения и обработки ресурсов поставщика ОВ, в отличие от модели локального размещения ПО, в которой расходы на аппаратно-программное обеспечение полностью ложатся на пользователя. В свою очередь, поставщик ОВ имеет возможность сфокусироваться на обслуживании только своей платформы (ЦОД): задача обслуживания пользовательского ПО на поставщика не возлагается. Подобная специализация (разделение зон ответственности) и обуславливает очевидную и подтверждённую практикой выгоду, выраженную в снижении издержек, для всех участников процесса. При этом решение многих задач конфигурирования ресурсов в рамках модели хорошо поддаётся автоматизации путём сведения типовых конфигураций в заранее сформированные пакеты услуг, например:

1. SaaS («ПО как услуга» – аренда ИТ-приложений);
2. PaaS («платформа как услуга» – разработка новых решений на базе облачных платформ);
3. DaaS («рабочее место как услуга» – аренда виртуального рабочего места);
4. IaaS («инфраструктура как услуга» – аренда ИТ-инфраструктуры).

Таким образом, основной побудительной силой развития данной технологии является возможность экономии ресурсов. В то же время, разумеется, нельзя утверждать, будто ОВ являются универсальным ответом на любые вызовы современной ИТ, поскольку до сих пор остаётся нерешённым множество вопросов, связанных с обеспечением отказоустойчивости (надёжности) облачных вычислений. ОВ активно завоёвывают рынок как в России, так и во всём мире. Однако, как и в отношении любой относительно свежей технологии, в отношении ОВ также имеются некоторые опасения, связанные не только с очевидно рекламным характером заявлений поставщиков услуг ОВ, но и с объективными рисками переноса чувствительной для бизнеса информации на удалённые серверы, поскольку бизнес справедливо расценивает данные как критичный с точки зрения своей жизнеспособности актив [6]. Совокупность указанных проблем и обуславливает актуальность настоящей работы.

Условимся понимать под технической надёжностью способность рассматриваемой системы обеспечивать заданные параметры функционирования на заданном интервале времени [5]. Надёжность является комплексной характеристикой, конкретное значение которой определяется как методом её оценки, так и качеством исходных данных. Опишем особенности функционирования ЦОД в рамках рассматриваемой модели, влияющие на составляющие надёжности ОВ.

Различают следующие основные варианты организации ОВ (таблица 1):

Табл. 1. Основные варианты организации ОВ

Вид	*Характеристика*
Частное (Private cloud)	*ОВ реализуются на аппаратно-программных ресурсах, имеющихся в распоряжении компании-пользователя. Цель разработки системы – обслуживание нужд одной организации. Управление в данной системе может осуществляться внутренними специалистами и/или внешним подрядчиком.*
Общее (Community cloud)	*В данной модели предполагается совместное использование облачной инфраструктуры несколькими организациями. Характерно наличие общих принципов, таких как: задачи, требования к безопасности, политики доступа и управления и тп. Управление осуществляется одной из организаций либо совместно, а также с привлечением внешнего подрядчика.*
Гибридное (Hybrid cloud)	*Для гибридной облачной инфраструктуры характерно сочетанием двух и более облаков (частных, общих или публичных), остающихся уникальными сущностями. Правила объединения стандартизированы. Обеспечивается переносимость данных и приложений между отдельными составляющими системы.*
Публичное (Public cloud)	*Инфраструктура ОВ доступна для большой группы потребителей, не связанных общими интересами. Инфраструктура принадлежит организации, которая продает либо предоставляет бесплатно соответствующие услуги.*

Как правило, инфраструктура ОВ предполагает использование более, чем единственного сервера. При этом данные, хранящиеся в облаке, распределяются

между несколькими серверами автоматически и прозрачно для пользователя; такой подход ориентирован как балансировку загрузки отдельных серверов, так и на минимизацию вероятности потери данных. Другим методом обеспечения отказоустойчивости в современных ОВ является периодическое сохранение состояния вычислительных процессов на основе т. н. «контрольных точек» (snapshot). Данный метод позволяет восстанавливать состояние процессов в случае отказа, при этом процессы обмениваются сообщениями для контроля состояний друг друга (рис.1):

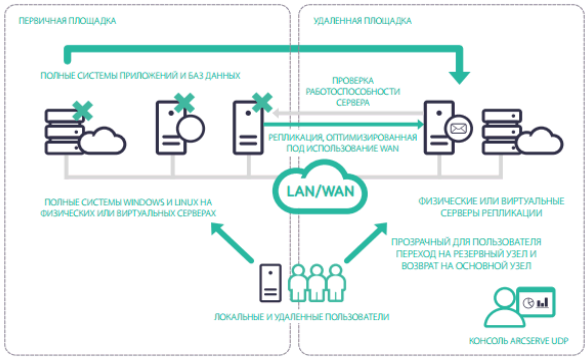

Рис. 1. Метод обеспечения отказоустойчивости путём сохранения состояний процесса

Отказоустойчивость в данной модели основывается на повышении индивидуальной надёжности каждого отдельного вычислительного узла. Поскольку каждый из процессов выполняется в рамках изолированной среды (виртуальной машины), для наблюдения за состоянием процесса используется специализированный программный модуль, расположенный вне исследуемой виртуальной машины и отвечающий за корректность её работы. Внешнее относительно обеспечиваемого процесса расположения модуля гарантирует отсутствие искажающих воздействий на собственно процесса, а накопленные эвристики (либо произвольно заданный график проверок) позволяют принимать решение о создании очередной контрольной точки. Восстановление системы предполагает откат состояния вычислительного процесса к последней заведомо корректной контрольной точке.

Другим способом организации отказоустойчивой работы ОВ является использование метода сохранения сообщений. Метод основывается на предположении (корректном в большинстве практических случаев), что любое изменение состояния всей системы может быть описано как последовательность сообщений, каждое из которых меняет состояние одного из компонентов системы. Такие сообщения асинхронно (без влияния на сам вычислительный процесс) фиксируются в виде очереди, расположенной в отдельной области памяти, что позволяет восстанавливать состояние системы после сбоев путём воспроизведения сохранённых сообщений.

Любой из существующих алгоритмов предполагает использование алгоритма-арбитра, внешнего по отношению к любой из обслуживаемых виртуальных машин и принимающего решения по их обслуживанию (рис.2):

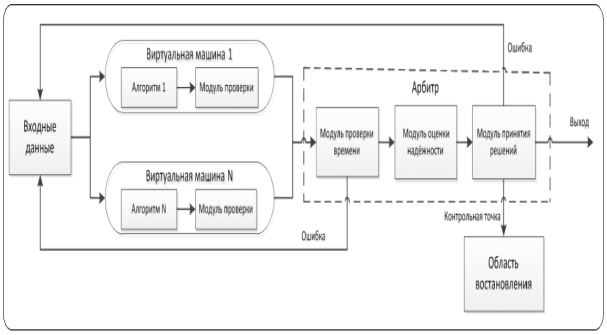

Рис. 2. Модель отказоустойчивости с использованием арбитра

Методы обеспечения надёжности отдельных компонентов ЦОД могут различаться (RAID-массивы, системы резервного копирования и проч.), но любой из них так или иначе сводится к резервированию (дублированию) аппаратно-программных ресурсов, обслуживающих вычислительные процессы. Это хорошо согласуется с положениями теории надёжности [5], которая прямо утверждает, что надёжность есть резервирование. Отметим, что, вообще говоря, дублирование данных увеличивает вероятность утечки конфиденциальной информации [6], но этот аспект выходит за рамки настоящей работы.

Рассмотрим укрупнённые схемы возможного взаимодействия между поставщиком (поставщиками) услуги ОВ и потребителем этой услуги (рис. 3):

$$[О] \rightarrow [Д] \rightarrow [П] \qquad (а)$$

$$[О_1] \rightarrow [Д_1] \rightarrow [П] \leftarrow [Д_2] \leftarrow [О_2] \qquad (б)$$

Рис. 3. Схема взаимодействия узлов в рамках модели ОВ

Здесь *О*– поставщик услуги; *П*– потребитель услуги; *Д*– канал передачи данных. Схема *а* соответствует единственному поставщику; схема *б*– варианту с более чем одним поставщиком.

Внимательное рассмотрение схемы рис. 3 приводит нас к парадоксальному на первый взгляд выводу: *любые усилия поставщиков услуг ОВ приводят лишь к относительно незначительному уменьшению ненадёжности всей схемы относительно потребителя*. В самом деле, обозначим вероятность отказа *i*-того элемента схемы как q_i [2]. Тогда вероятность безотказной работы будет определяться как $p_i=1-q_i$. Вероятность безотказной работы последовательно соединённых

элементов (всей системы *S*) определяется как произведение индивидуальных вероятностей:

$$P_S=p_1*p_2*...*p_n, \quad (1)$$

где *n*– общее количество элементов системы. Поскольку каждый из множителей в формуле (1) меньше 1, общая надёжность системы с точки зрения потребителя снижается тем сильнее, чем больше элементов в цепочке между потребителем и поставщиком. Это рассуждение может показаться не слишком существенным, поскольку структурное резервирование схемы *б* рис. 3 предполагает не последовательный, а параллельный характер соединения элементов, однако в подавляющем большинстве реальных случаев гипотетические элементы *Д1..Дn* являются одним и тем же физическим провайдером услуг связи, который таким образом *при любом распределении вычислительных процессов по раздельным ЦОД* становится единственной точкой отказа, показатели которой заведомо доминируют во вкладах в ненадёжность. По нашему мнению, общая картина носит ещё более пессимистичный характер, поскольку в ней присутствуют также плохо формализуемые и слабо прогнозируемые факторы, такие как политически и экономически мотивированные санкции, возможные решения об изоляции отдельных сегментов всемирной сети, военные конфликты (Ирак, Сирия, Ливия и т.д.) и прочее. Таким образом, при выборе инфраструктуры ОВ пользователю не следует руководствоваться лишь рекламными заявлениями поставщиков соответствующих услуг, но рассматривать картину в целом, с учётом текущей и перспективной доступности удалённых сервисов.

Основные выводы по работе:

1. Современное состояние ОВ предлагает возможность построения информационной инфраструктуры практически любой разумной конфигурации. При этом гарантируется высокая эластичность использования вычислительных ресурсов и простота управления ими.

2. В большинстве случаев размещение вычислительных задач в инфраструктуре ОВ является финансово выгодным по сравнению с созданием локальной инфраструктуры.

3. Вопрос отказоустойчивости и безопасности доступа к сервисам ОВ следует рассматривать комплексно, с обязательным учётом транспортных возможностей сети, а также рисков не технического характера.

4. Вопрос оценки общесистемной надёжности инфраструктуры ОВ относительно потребителя представляет собой слабоизученную тему, представляющую значительный интерес с т.з. как дальнейшей формализации исходных показателей надёжности (узловое и промежуточное оборудование, ПО, человеческий фактор, социальный фактор), так и собственно методов такой оценки.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Аленова Н.М. Облачные вычисления. – М., 2013. 361 с.

2. Вентцель Е.С., Овчаров Л.А. Теория случайных процессов и её инженерные приложения: Учеб. пособие для втузов. / Вентцель Е.С. – 2-е изд. , стер. – М.: Высш. шк., 2012. – 383 с.

3. Глушков В.М. Основы безбумажной информатики. М.: Наука, 1982. – 362 с.

4. Китов А.И. Электронные цифровые машины. М.: Советское радио, 1956. – 358 с.

5. Райншке К., Модели надёжности и чувствительности систем. М.: Мир, 1979. – 452 с.

6. Белов Д.А., Давлекамова И.А. Защита персональных данных при переходе к облачным вычислениям // Современные научные исследования и инновации. 2017. №5 [электронный ресурс]. – Режим доступа: http://web.snauka.ru/issues/2017/05/82443 (дата обращения: 29.11.2017).

7. https://cloud.google.com/ [электронный ресурс]. – Режим доступа: https://cloud.google.com/ (дата обращения 25.04.2019).

8. https://www.it-grad.ru/ [электронный ресурс]. – Режим доступа: https://www.it-grad.ru/ (дата обращения 25.04.2019).

9. https://aws.amazon.co [электронный ресурс]. – Режим доступа: https://aws.amazon.com (дата обращения 25.04.2019).

10. https://azure.microsoft.com [электронный ресурс]. – Режим доступа: https://azure.microsoft.com (дата обращения 25.04.2019).

Судани Хайдар Хуссейн – аспирант, Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского, Министерство науки и технологий Ирака, Багдад, Ирак.

Михаил Борисович Абросимов – д.ф.-м. н, доцент, заведующий кафедрой теоретических основ компьютерной безопасности и криптографии Саратовского национального исследовательского государственного университета имени Н.Г. Чернышевского, Саратов.

FAULT TOLERANCE AND SECURITY OF ACCESS IN CLOUD COMPUTING

H.H. Sudani [1], M.B. Abrosimov[2]

[1]*Saratov National Research State University named after N.G. Chernyshevsky, Ministry of Science and Technology of Iraq, Baghdad, Iraq*

[2]*Saratov National Research State University named after N.G. Chernyshevsky, Saratov*

Abstract: The key issues related to the organization of the infrastructure of cloud technologies are considered. The main types of «clouds» and the principles of their work are described, the main approaches to ensuring the resiliency of cloud systems, including features of methods for restoring the system after failures based on the preservation of process states, are shown. The question of a comprehensive assessment of the reliability of the cloud computing infrastructure is formulated, the main problems and merits of the "cloud computing" are indicated.

Results achieved: the main aspects of the functioning of providers and consumers of cloud computing services are described, the features of their interrelations and the systemic nature of the issue are shown. The task of complex assessment of the reliability of the relevant infrastructure is formulated.

Keywords: *infrastructure, cloud computing, data centers, fault tolerance, reliability, virtualization*

REFERENCES

1. Alenova N.M. Cloud computing. - M., 2013. 361 c.
2. Wentzel, E.S., Ovcharov, L.A. Theory of random processes and its engineering applications: Proc. manual for technical colleges. / Wentzel E.S. - 2nd ed. - M.: Higher. Sc., 2012. - 383 p.
3. Glushkov V.M. Basics of paperless computer science. M .: Science, 1982. - 362 p.
4. Kitov A.I. Electronic digital machines. M .: Soviet Radio, 1956. - 358 p.
5. Reinshke K., Models of reliability and sensitivity of systems. M .: Mir, 1979. - 452 p.
6. Belov D.A., Davlekamova I.A. Protection of personal data in the transition to cloud computing // Modern scientific research and innovation. 2017. №5 [electronic resource]. - Access mode: http://web.snauka.ru/issues/2017/05/82443 (access date: 11/29/2017).
7. https://cloud.google.com/ [electronic resource]. - Access mode: https://cloud.google.com/ (request date 04/25/2019).
8. https://www.it-grad.ru/ [electronic resource]. - Access mode: https://www.it-grad.ru/ (request date 04/25/2019).
9. https://aws.amazon.co [electronic resource]. - Access mode: https://aws.amazon.com (the date of appeal is 04/25/2019).
10. https://azure.microsoft.com [electronic resource]. - Access mode: https://azure.microsoft.com (the date of the appeal is 04/25/2019).

Sudani Hayder Hussein – graduate student, Saratov National Research State University named after N.G. Chernyshevsky, Ministry of Science and Technology of Iraq, Baghdad, Iraq.

M.B. Abrosimov2 Ph.D., associate professor, head of the department of the theoretical foundations of computer security and cryptography at the Saratov National Research State University named after N.G. Chernyshevsky, Saratov.